EnGenius®Work & Play Series®

Wireless-N Gigabit Router
User Guide

V1.0

TABLE OF CONTENTS

Product Overview

Product Overview 1-1
Package Contents 1-2
Product Layout 1-3
LEDs 1-3
Back Panel Components 1-4

Installation

System Requirements 2-1
Wall Mounting 2-2

EnGenius Quick Start

Installing the Software 3-1
Setup Notes 3-1

Installation 3-1
Connecting Network Cables 3-3

Web Configuration

Logging In 4-1
Viewing the Dash Board 4-2
Services 4-3
Home 4-3
Setup Wizard 4-3
Network Settings 4-3
Language 4-3
Logout 4-3
Web Menus Overview 4-4
System 4-4
Internet 4-5
Wireless 4-6
Guest Network 4-7
IPv6 4-8
Firewall 4-9

Advanced 4-10
Tools 4-11

Installation Setup Wizard

Detecting the Internet Connection 5-1

Basic Network Settings

System Setup 6-1
Viewing System Status 6-1
System 6-1
WAN Settings 6-2
LAN Settings. 6-3
Wireless 6-3
Guest Network 6-4
Configuring Operation Mode 6-5
Router Mode 6-5
Repeater Mode 6-5
Configuring LAN 6-6
LAN IP 6-6

DHCP Server. 6-7
DNS Server 6-8
Configuring DHCP 6-9
DHCP Client Table 6-9
Enable Static DHCP IP 6-9
Current Static DHCP Table 6-10
Configuring Logging 6-11
Log Message List. 6-11
Monitoring Bandwidth Usage 6-12
Configuring Languages 6-13
Configuring WAN Settings 6-14
View WAN Status 6-14
WAN Settings 6-14
Configuring Dynamic IP 6-15
Dynamic IP. 6-15
DNS Servers 6-16
Configuring Static IP 6-17
Static IP. 6-17
Configuring PPPoE 6-18

Configuring PPTP 6-20
WAN Interface Settings 6-20
Dynamic IP Address 6-20
PPTP Settings 6-21
Configuring L2TP 6-22
WAN Interface Settings 6-22
Dynamic IP Address 6-22
L2TP Settings 6-23
Configuring DS-Lite 6-24
Wireless LAN Setup 6-25
Configuring Basic Settings 6-25
Access Point Mode 6-26
Wireless Distribution System Mode 6-27
Configuring Advanced Settings 6-30
Configuring Security 6-32
Encryption Type 6-33
Wired Equivalent Privacy (WEP) 6-33
Encryption: Wi-Fi Protected Access (WPA) Pre-Shared Key 6-34
Encryption: WPA RADIUS 6-35

Configuring Filter 6-36
Enable Wireless Access Control 6-36
MAC Address Filtering Table 6-37
Configuring Wi-Fi Protected Setup 6-38
Configuring Client List 6-39
Guest Network 6-40
Enabling Guest Network 6-40
Configuring Guest IP Address 6-41
Viewing Guest Client List 6-42
IPv6 6-43
View IPv6 Status 6-43
Static IPv6 6-44
Configure Autoconfiguration 6-45
Configure PPPoE 6-46
Configuring 6to4 6-48
Configure 6RD 6-49
Configure Link-Local 6-51
Firewall Setup 6-52

Configure Basic Settings 6-52
Configuring Advanced Settings 6-53
Configuring Demilitarized Zone 6-54
Configuring Denial of Service 6-55
WAN Settings 6-55
Configure MAC Filter 6-56
Configure IP Filter 6-57
URL Filtering 6-58
Advanced Network Settings 6-59
NAT Setup 6-59
Port Mapping Setup 6-60
Port Forwarding Setup 6-62
Port Triggering Setup 6-64
Application Layer Gateway Setup 6-66
Universal Plug and Play Setup 6-67
Internet Group Multicast Protocol Setup 6-68
Quality of Service Setup 6-69
Priority Queue. 6-70

Bandwidth Allocation 6-71
Routing Setup 6-72
Wake on LAN Setup 6-74
Tools Setup 6-75
Configuring the Administrator Account 6-75
Configuring the Router’s Time 6-76
Configuring DDNS 6-77
Diagnosing a Network Connection 6-78
Upgrading Firmware 6-79
Backing Up Settings 6-80
Rebooting the Device 6-81

Appendix A

Federal Communication Commission Interference Statement 6-82

Appendix B

Industry Canada Statement 6-84

Appendix C

Link Layers 6-85
Dynamic IP Address (DHCP) 6-85
Static IP 6-85
Point-to-Point Protocol over Ethernet (PPPoE) 6-86
Layer 2 Tunneling Protocol (L2TP) 6-86

Appendix D

WorldWide Technical Support 6-87

Copyright

This user guide and its content is copyright of © EnGenius Networks, 2012. All rights reserved.

Any redistribution or reproduction in part or in whole in any form is prohibited.

Do not distribute, transmit, store in any form of electronic retrieval system or commercially exploit the content without the expressed written permission of EnGenius Networks.

Conventions

The following conventions are used to give the user additional information about specific procedures or content. It is important to pay attention to these conventions as they provide information to prevent damage to equipment or personal injury.

General Conventions

The following general conventions are used in this document.

CAUTION!

CAUTIONS APPEAR BEFORE THE TEXT IT REFERENCES. CAUTIONS APPEAR IN CAPITAL LETTERS TO EMPHASIZE THAT THE MESSAGE CONTAINS VITAL HEALTH AND SAFETY INFORMATION.

WARNING!

Warning information appears before the text it references to emphasize that the content may prevent damage to the device or equipment.

Important:

Indicates information that is important to know for the proper completion of a procedure, choice of an option, or completing a task.

Note:

Indicates additional information that is relevant to the current process or procedure.

Example:

Indicates information used to demonstrate or explain an associated concept.

N/A:

Indicates that a component or a procedure is not applicable to this model.

Prerequisite:

Indicates a requirement that must be addressed before proceeding with the current function or procedure.

Typographical Conventions

The following typographical conventions are used in this document:

Italics

Indicates book titles, directory names, file names, path names, and program/process names.

`Constant width`

Indicates computer output shown on a computer screen, including menus, prompts, responses to input, and error messages.

`Constant width bold`

Indicates commands lines as entered on the computer. Variables contained within user input are shown in angle brackets (< >).

Bold

Indicates keyboard keys that are pressed by the user.

Product Overview

1.1 Product Overview

Thank you for purchasing the ESR9850v2 Wireless-N Gigabit Router from EnGenius Networks.

The EnGenius ESR9850v2 Wireless-N Gigabit Router is a member of the EnGenius Work & Play series of routers.

The ESR9850v2 offers 1 WAN and 4 LAN Gigabit connections and extender signal coverage with two external high sensitive 2dBi detachable antennas. The ESR9850v2 also feature wireless easy setup – WPS function. It helps user to connect to wireless device with just one push button.

The ESR9850v2 provides advanced security features to protect your network and the devices connected to it. An SPI Firewall protects the LAN as well as data sent over the Internet. Data encryption protocol, such as WEP, WPA, WPA2 and MAC address Filtering are some of the other features which block access from unauthorized clients and better manage Wi-Fi accessibility.

The ESR9850v2 supports the next generation IPv6 (Internet Protocol version 6) to enable highly reliable applications and enhanced security for safer Internet connectivity.

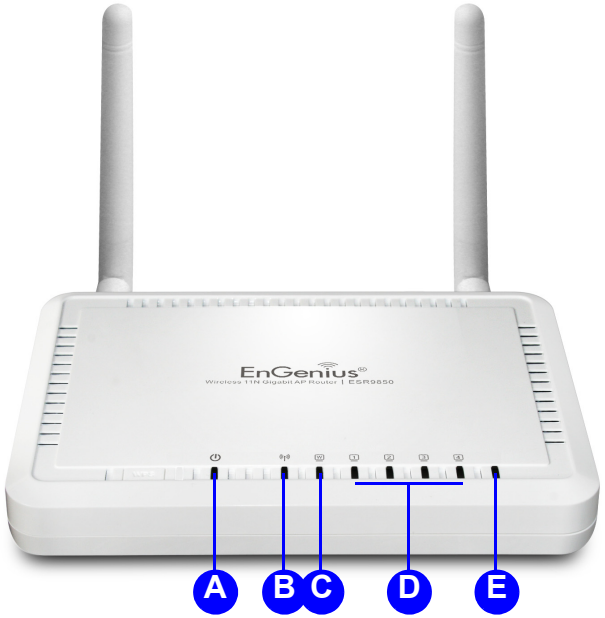
- High Performance Gigabit Connection
- QoS Wireless Multi-Media (WMM)
- Wireless LAN Power Saving
- SPI Firewall / DoS Protection
- Guest Network
- Hardware NAT
- IPv6 Compliance

1.1 Package Contents

ITEM	QUANTITY
Wireless-N Gigabit Router	1
2dBi Antenna	2
Quick Installation Guide	1
12V/1A Power Adapter	1
Ethernet Cable	1
User CD (with user manual)	1
Technical Support Card	1

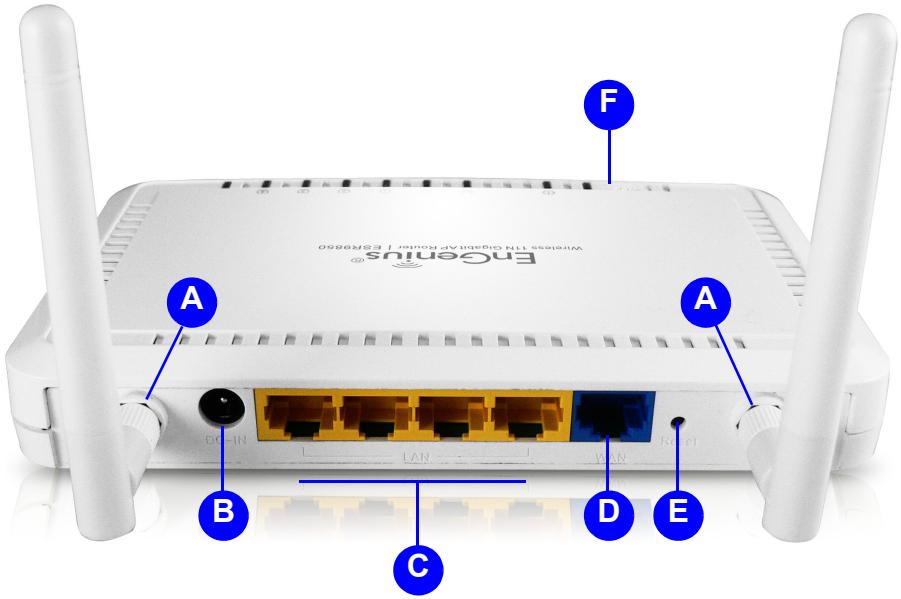
1.1 Product Layout

LEDs



	LED	DESCRIPTION
A	Power/Status	Power status LED
B	WLAN	Wireless LAN (WLAN) status LED
C	WAN	Internet connection status LED
D	LAN (1 – 4)	LAN port status LED(s)
E	WPS	WPS status LED

Back Panel Components



	BACK PANEL COMPONENTS	DESCRIPTION
A	External Antenna Connectors	SMA Connectors
B	DC Power Jack	Connects the router to a DC power adapter source
C	LAN Ports (1 – 4)	10/100/1000Mbps Ethernet/ RJ-45
D	WAN Port	10/100/1000Mbps Ethernet/ RJ-45
E	Reset Button	• 10 seconds for reboot • 10~15 seconds for reset to factory default
F	WPS Push Button	Wi-Fi Protected Setup

Installation

2.1 System Requirements

To install the ESR9850v2, you need the following:

- Computer (Windows, Linux and MAC OS X Operating Systems)
- CD-ROM
- Web Browser (Internet Explorer, FireFox, Chrome, Safari)
- Network Interface Card with an open RJ-45 Ethernet Port
- Wi-Fi Card or USB Wi-Fi Dongle (802.11 B/G/N)
- xDSL, Cable Modem or Fiber Modem
- RJ45 Ethernet Cables

2.1 Wall Mounting

Mounting the ESR9850v2 on a wall optimizes the wireless access range.

Note:
Choose a location that is within reach of an electrical outlet for the AC adapter and the DSL or Cable modem.

To mount the device on the wall do the following:

1. Measure the distance from the middle of each mounting screw hole.
2. Mark the locations of the screw holes on the wall.
3. Drill a hole for each marked location and insert a screw in each.

Note:
Make sure to leave enough of the screw head above the wall surface to secure the router.

4. Install and secure the mounts onto the ESR9850v2.
5. Install the ESR9850v2 on the wall.

EnGenius Quick Start

3.1 Installing the Software

Note:
Before getting started, please power off the cable or DSL modem.

Setup Notes

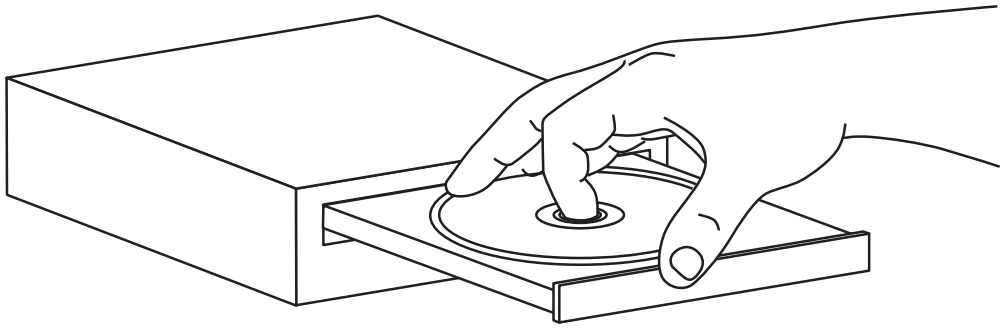
When considering the placement of the ESR9850v2 remember the following:

- It must be located close to a DSL or Cable modem.
- It must be close to an electrical outlet.
- Upon first setup, it must be close to the computer that is used to set up and configure the router.
- For optimal wireless access place the router in the center of the room, at a high altitude and with an unobstructed view of the other wireless devices.
- Other electronic devices can interfere with the wireless frequency of the router and reduce the wireless access range.

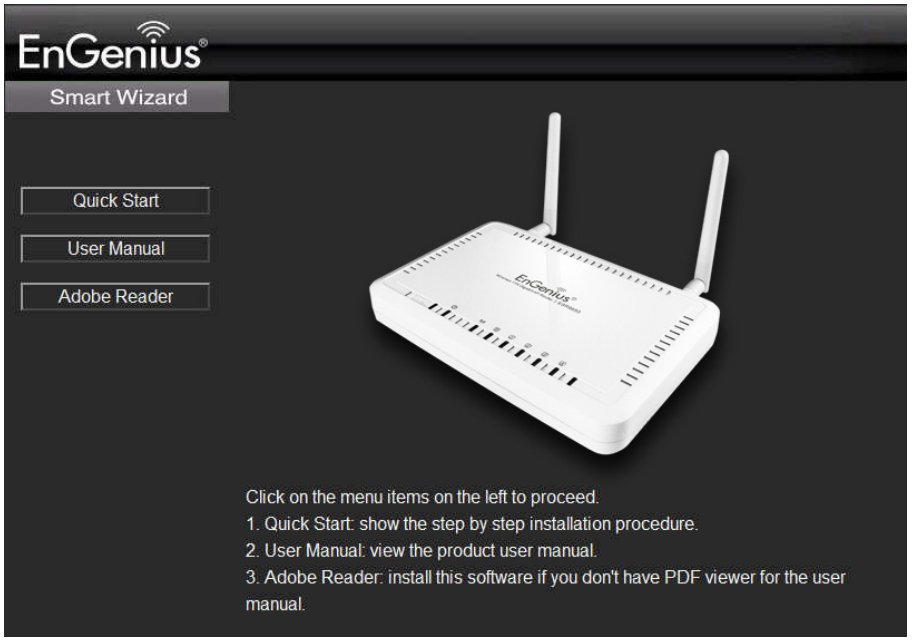
Installation

Note:
If the instructions do not automatically start, open a file manager and browse the root folder of the CD-ROM. Look for the file named *index.html* and open it.

1. Insert the ESR9850v2 installation CD into the CD-ROM drive.



2. Click **Quick Start**. The wizard will guide you through setting up your ESR9850v2.

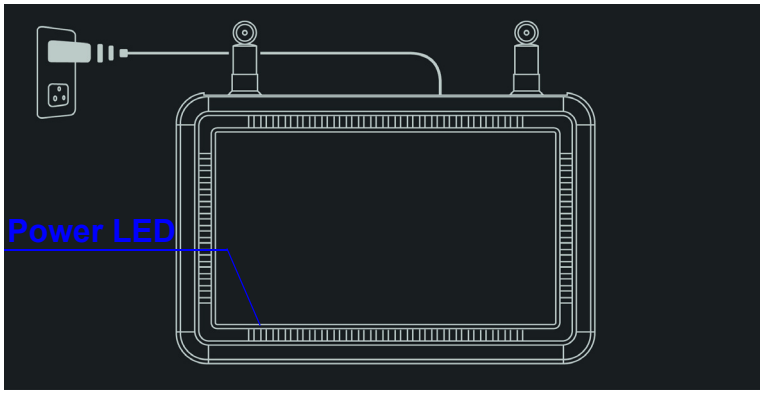

EnGenius
Smart Wizard
Quick Start
User Manual
Adobe Reader
Click on the menu items on the left to proceed.
1. Quick Start: show the step by step installation procedure.
2. User Manual: view the product user manual.
3. Adobe Reader: install this software if you don't have PDF viewer for the user manual.

3.1 Connecting Network Cables

CAUTION!

UNPLUG ALL PERIPHERALS AND THE ROUTER'S ADAPTER BEFORE STARTING WITH THIS PROCEDURE.

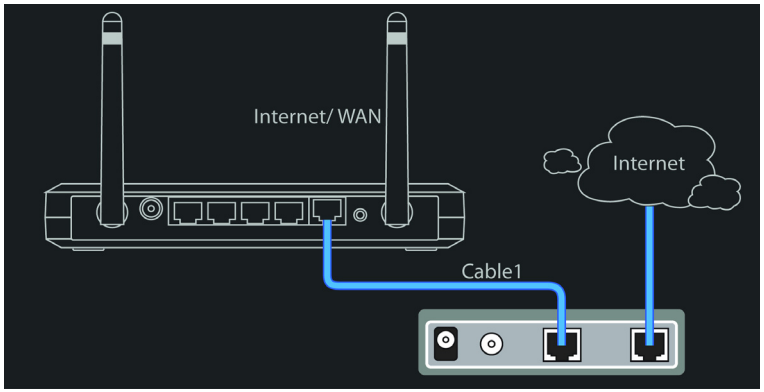
1. Connect the adapter cable to an electrical outlet.



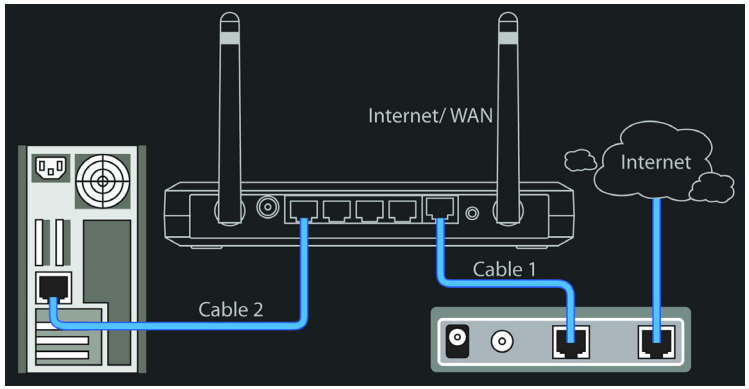
Note:

The Power LED lights up to show the device is active.

2. Plug one end of the Ethernet cable into the WAN port on the back panel of the router. Plug the other end of the cable into the cable or DSL modem.



3. Plug one end of an Ethernet cable into the LAN port on the back panel of the router. Plug the other end of the cable into the Ethernet port of the computer.
4. Click `Next` to display the login screen.



Note:
If the browser does not show the login screen, enter the default router IP address, **`192.168.0.1`**.

Note:
Make sure the network cable and power adapter are firmly connected.

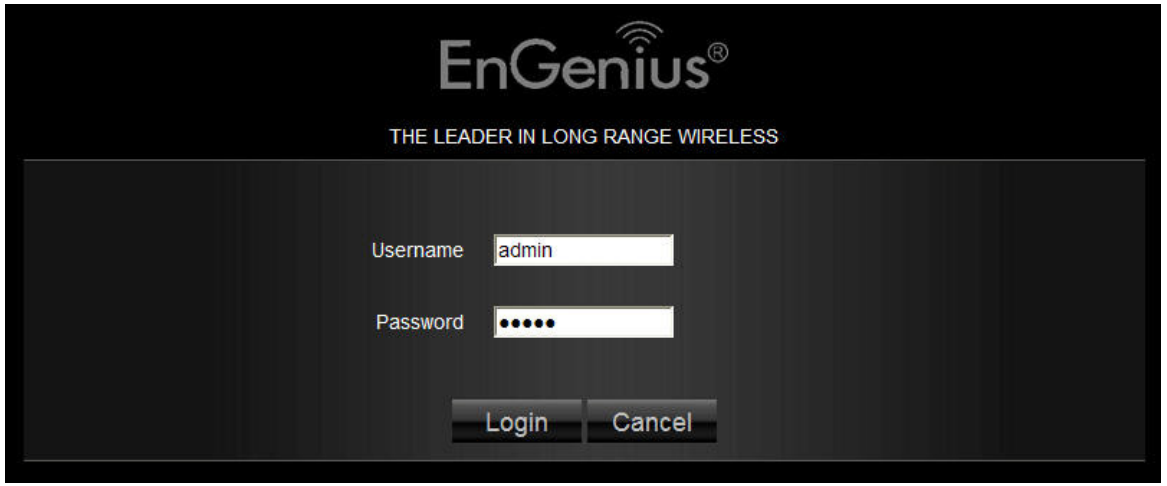
Web Configuration

4.1 Logging In

Note:
If the login screen does not display, enter the default router IP address of `192.168.0.1`.

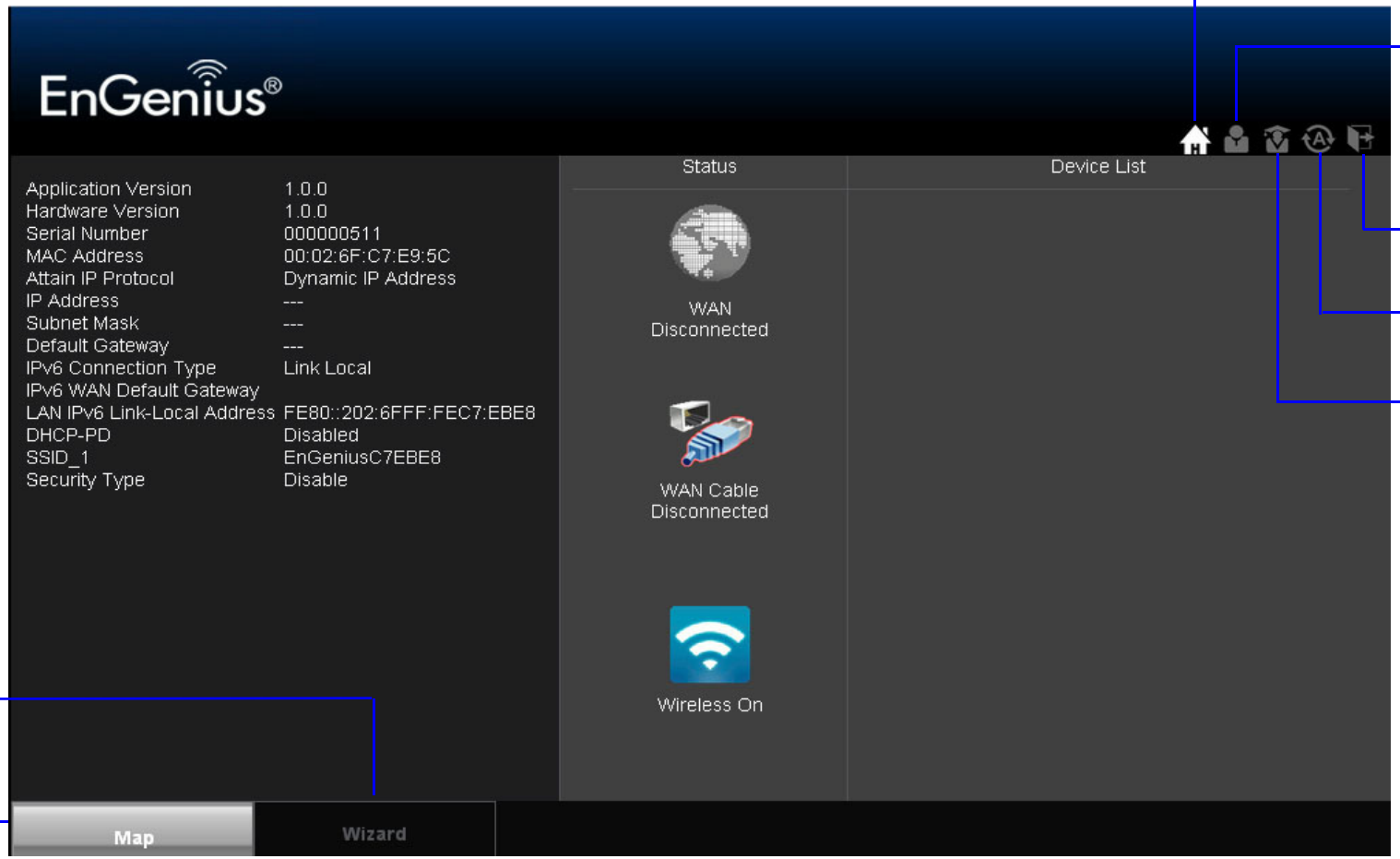
Note:
The default user name is **`admin`** and the default password is **`admin`**.

1. At the login screen enter a user name and a password.
2. Click `Login` to continue.



4.1 Viewing the Dash Board

The main screen, or dashboard, provides access to all of the router's services.



Services

The Home, Setup Wizard, Network Settings and Exit links are the main service areas.

Home

The Home link displays the dashboard screen.

Setup Wizard

The Setup Wizard link starts the wizard that automatically configures the router. Refer to “Detecting the Internet Connection” on page 5-1.

Network Settings

The Network Settings link displays the menus to manually configure the router. Refer to “Web Menus Overview” on page 4-4.

Language

The Language link displays the menu to set the OSD language. Refer to “Configuring Languages” on page 6-13.

Logout

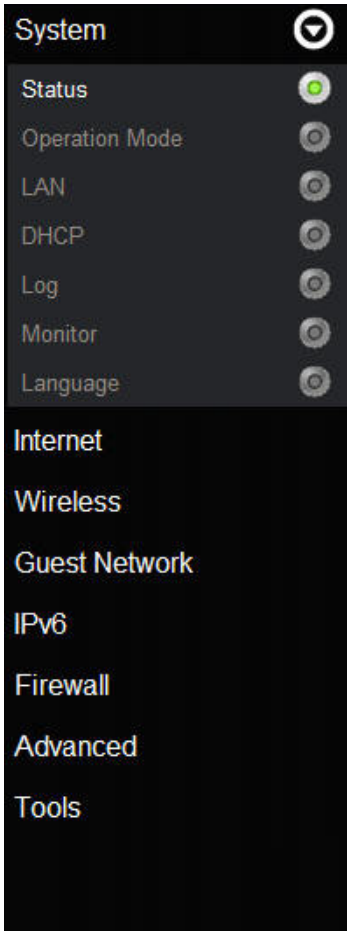
The Logout link closes the router configuration software.

4.1 Web Menus Overview

System

View and edit settings that affect system functionality

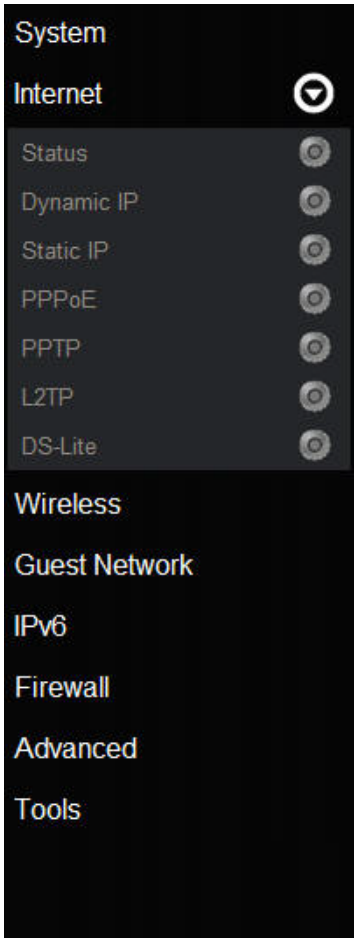
- **Status** Display the summary of the current system status.
- **Operation Mode** Sets the operator mode as either as an AP router or a Wireless Repeater.
- **LAN** Configure the wired network.
- **DHCP** Configure dynamically allocated IP addresses.
- **Log** View recorded system operations and network activity events.
- **Monitor** View the current network traffic bandwidth usage.
- **Language** Configure the application menu and GUI language.



Internet

View and edit settings that affect network connectivity

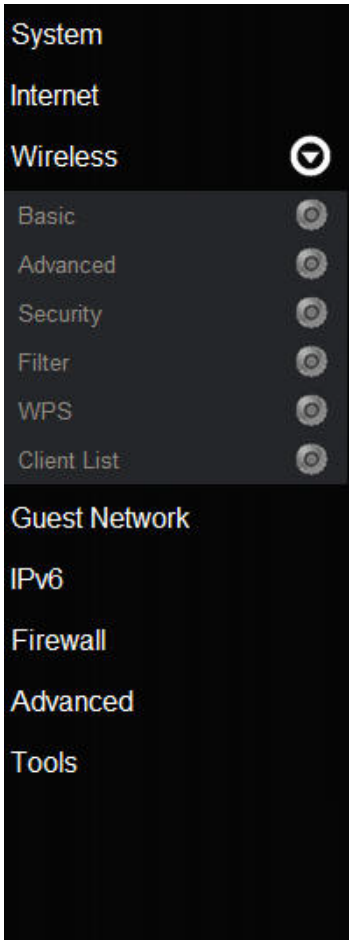
- **Status** Display the summary of the Internet status and type of connection.
- **Dynamic IP** Setup a dynamic IP connection to an Internet service provider (ISP).
- **Static IP** Setup a static IP connection to an ISP.
- **PPPoE** Setup a PPPoE connection to an ISP.
- **PPTP** Setup a PPTP connection to an ISP.
- **L2TP** Setup an L2TP connection to an ISP.
- **DS-Lite** Setup the IPv6 properties



Wireless

View and edit settings for wireless network connectivity.

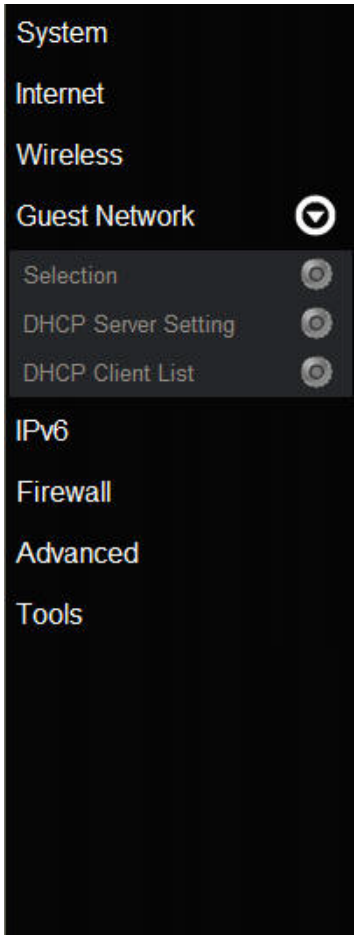
- **Basic** Configure the minimum settings required to setup a wireless network connection.
- **Advanced** Configure the advanced wireless network settings.
- **Security** Configure the wireless network security settings.
- **Filter** Configure a list of clients that are allowed to wirelessly connect to the network.
- **WPS** Automate the connection between the a wireless client and the router using an 8-digit PIN.
- **Client List** View the wireless devices currently connected to the network.



Guest Network

View and configure settings for guest network rule sets.

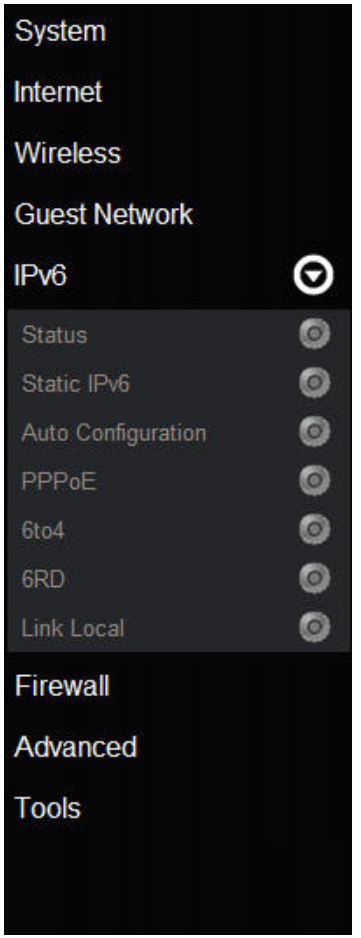
- **Selection** Enable or disable the Guest Network function.
- **DHCP Server Setting** Configure the Guest Network DHCP server settings.
- **DHCP Client List** Configure the Guest Network client list.



IPv6

View and configure settings for IPv6.

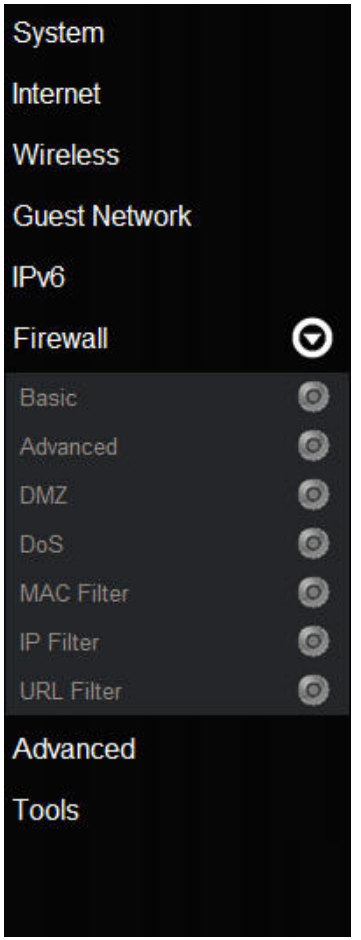
- **Status** Shows IPv6 LAN connection details.
- **Static IPv6** Set IPv6 address information provided by an Internet Service Provider (ISP).
- **Auto Configuration** IPv6 auto configuration settings.
- **PPPoE** Enter PPPoE IPv6 information provided by an Internet Service Provider (ISP).
- **6to4** Configure the IPv6 to IPv4 transition mechanism.
- **6RD** Configure the IPv6 rapid deployment mechanism.
- **Link Local** Configure the IPv6 link local address.



Firewall

View and configure settings for firewall rule sets.

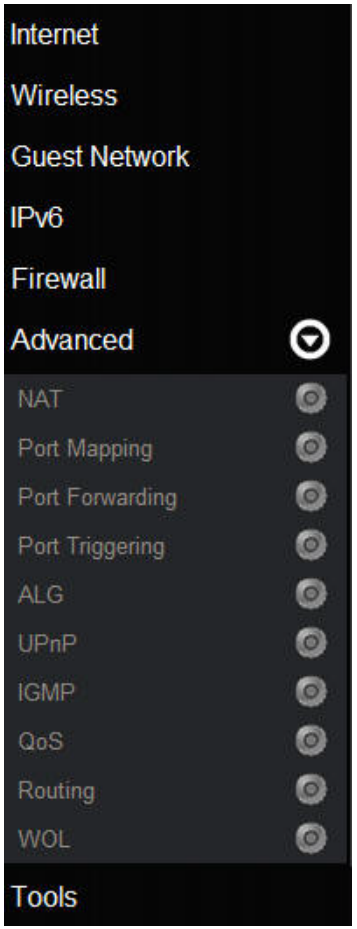
- **Basic** Enable or disable the network firewall.
- **Advanced** Configure virtual private network (VPN) packets.
- **DMZ** Redirect packets from the WAN port IP address to a particular IP address on the LAN.
- **DoS** Enable or disable blocking of denial of service (DoS) attacks.
- **MAC Filter** Configure MAC filters to deny or allow LAN computers from accessing the Internet.
- **IP Filter** Configure IP filters to deny or allow LAN computers from accessing the Internet.
- **URL Filter** Block access to certain Web sites for a particular PC by entering either a full URL address or just a keyword of the Web site.



Advanced

View and configure advanced system and network settings.

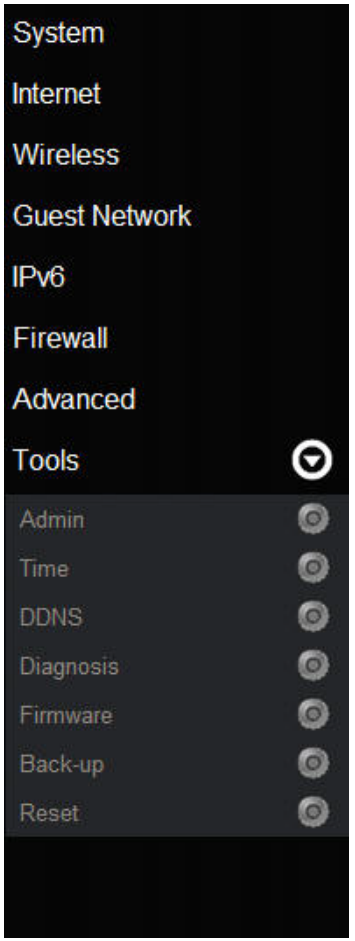
- **NAT** Enable or disable Network Address Translation (NAT).
- **Port Mapping** Re-direct a range of service port numbers to a specified LAN IP address.
- **Port Forwarding** Configure server applications to send and receive data from specific ports on the network.
- **Port Triggering** Configure applications that require multiple connections and different inbound and outbound connections.
- **ALG** Configure the application layer gateway (ALG).
- **UPnP** Enable or disable Universal Plug and Play (UPnP) functionality.
- **IGMP** Enable or disable the Internet Group Multicast Protocol (IGMP).
- **QoS** Configure the network quality of service (QoS) setting by prioritizing the uplink and downlink bandwidth.
- **Routing** Configure static routing.
- **WOL** Configure wake on LAN (WOL) to turn on a computer over the network.



Tools

View and configure system and network tools settings.

- **Admin** Configure the administrator password used to login to the router.
- **Time** Configure the system time on the router.
- **DDNS** Map a static domain name to a dynamic IP address.
- **Diagnosis** Check if a specific computer is connected to the LAN.
- **Firmware** Update the router's firmware.
- **Backup** Load or save configuration settings from a backup file or restore the factory default settings.
- **Reset** Manually reset the router.

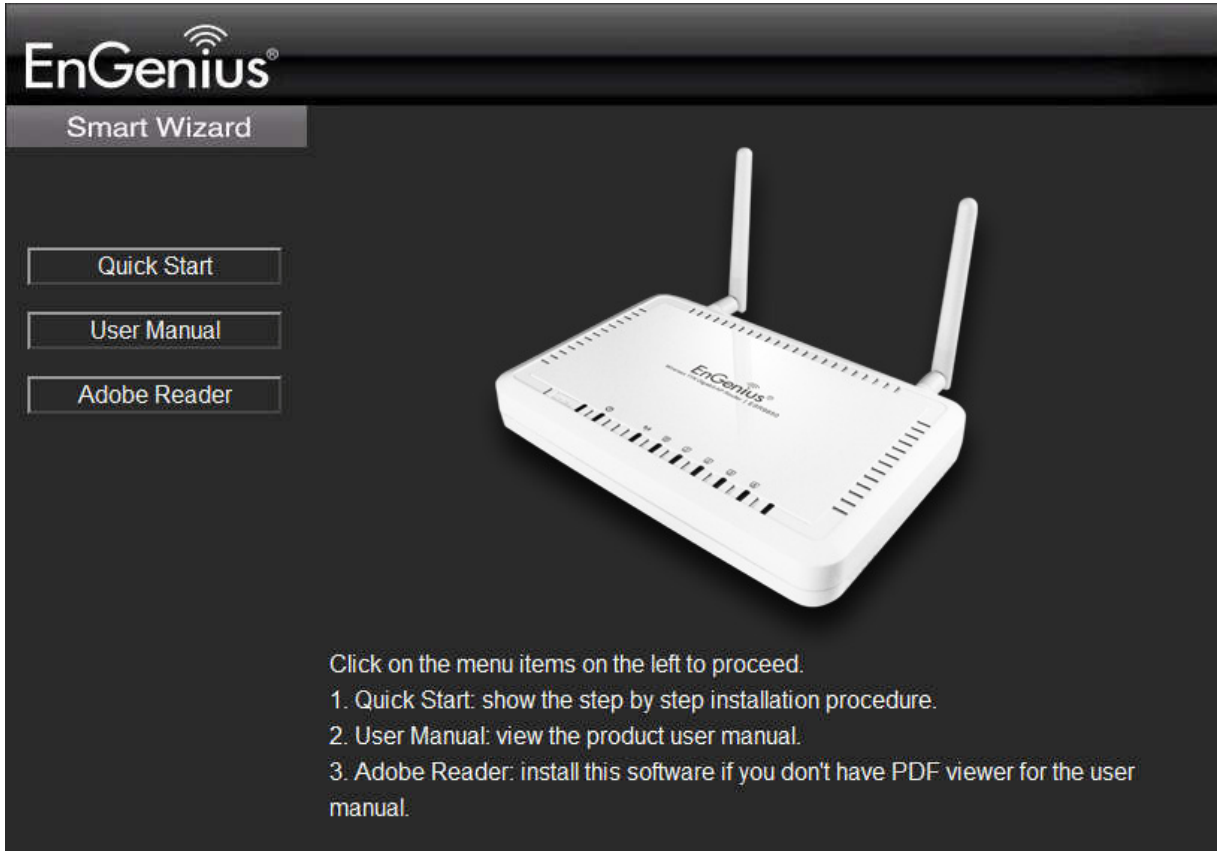


Installation Setup Wizard

5.1 Detecting the Internet Connection

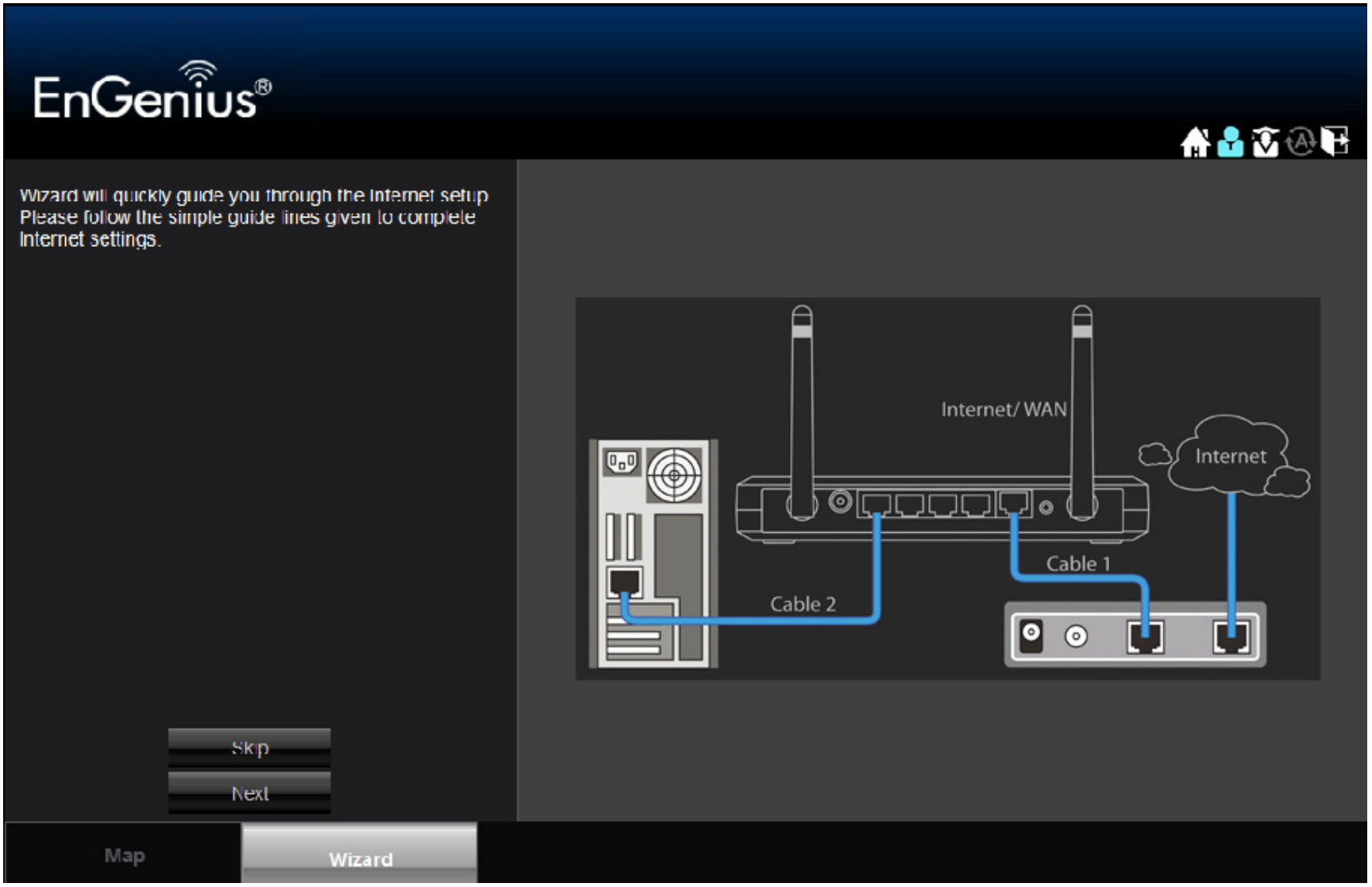
Use the Wizard to automatically detect the type of Internet connection.

1. Insert the ESR9850v2 Installation CD into your CD-ROM drive to display the EnGenius Smart Wizard screen.

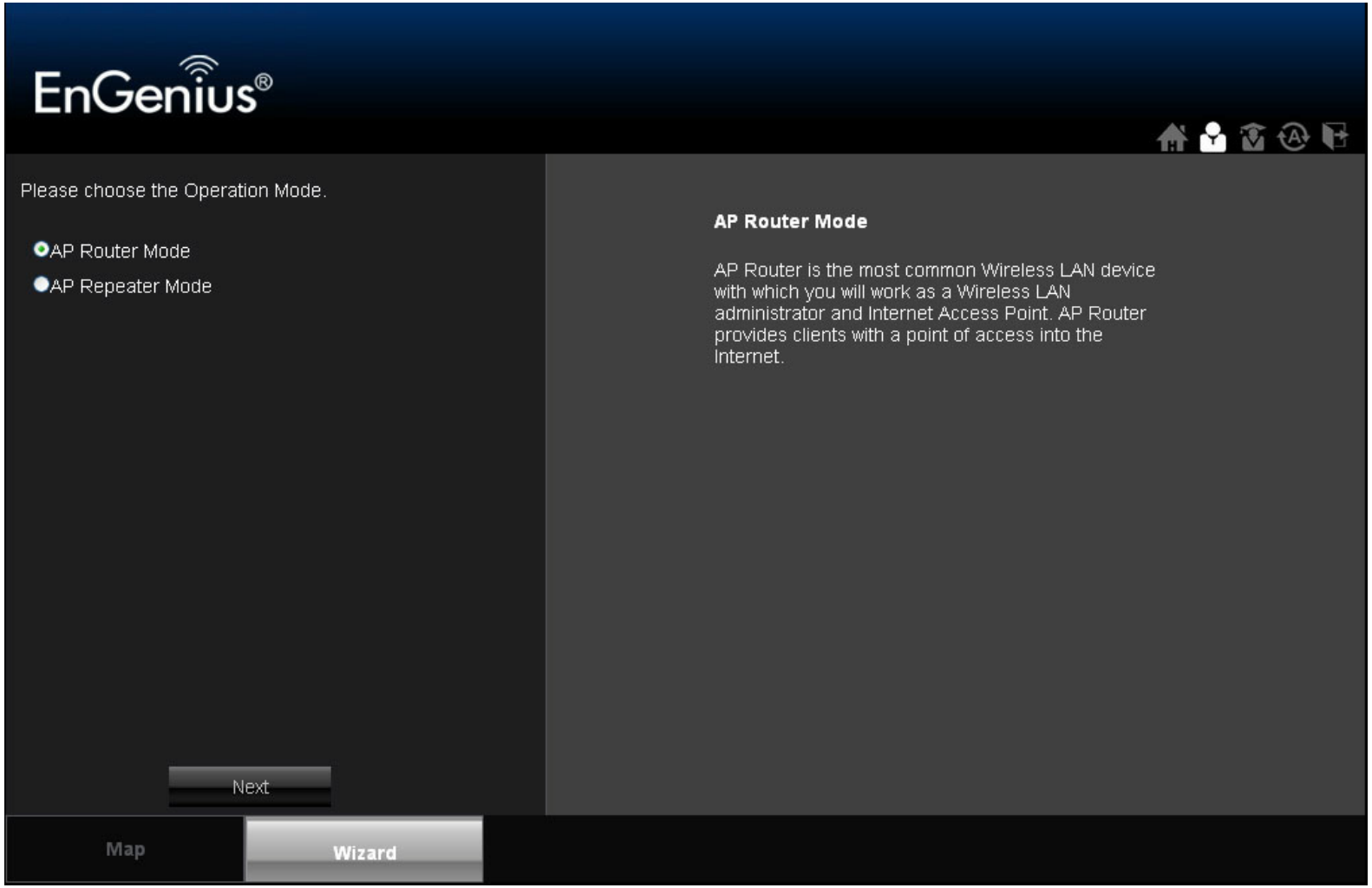

EnGenius
Smart Wizard
Quick Start
User Manual
Adobe Reader
Click on the menu items on the left to proceed.
1. Quick Start: show the step by step installation procedure.
2. User Manual: view the product user manual.
3. Adobe Reader: install this software if you don't have PDF viewer for the user manual.

2. Click `Quick Start` to continue an display the Wizard Introduction screen.

3. Click `Next` to continue or `Skip` to cancel the wizard.

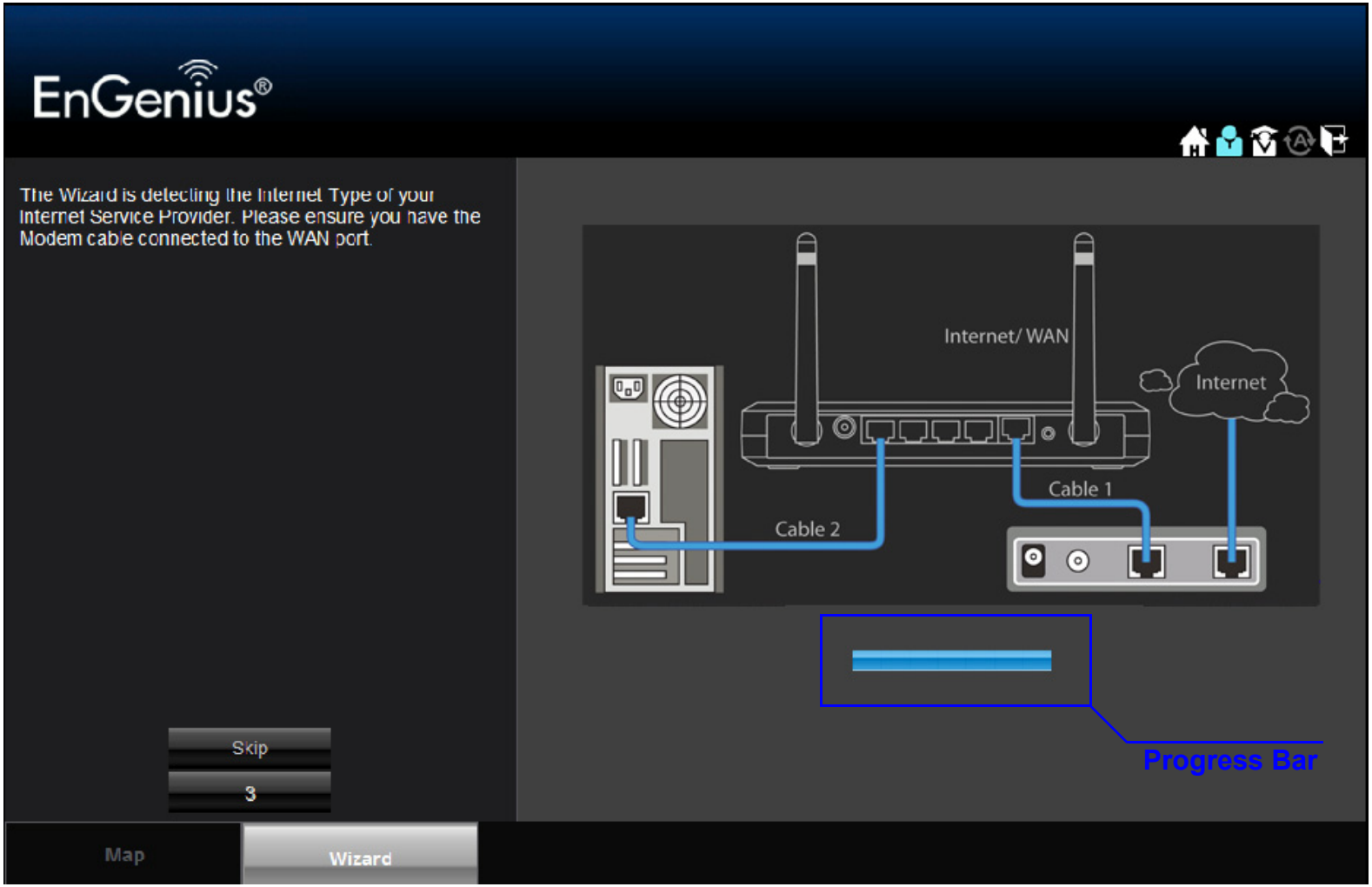


4. To choose an operation mode, perform one of the follow steps:
   - Click `AP Router Mode` and refer to *Detecting the Internet Connection in AP Router Mode* for the remaining steps.
   - Click `AP Repeater Mode` and refer to *Detecting the Internet Connection in AP Repeater Mode* for the remaining steps.


EnGenius®
Please choose the Operation Mode.
AP Router Mode
AP Repeater Mode
AP Router Mode
AP Router is the most common Wireless LAN device with which you will work as a Wireless LAN administrator and Internet Access Point. AP Router provides clients with a point of access into the Internet.
Next
Map
Wizard

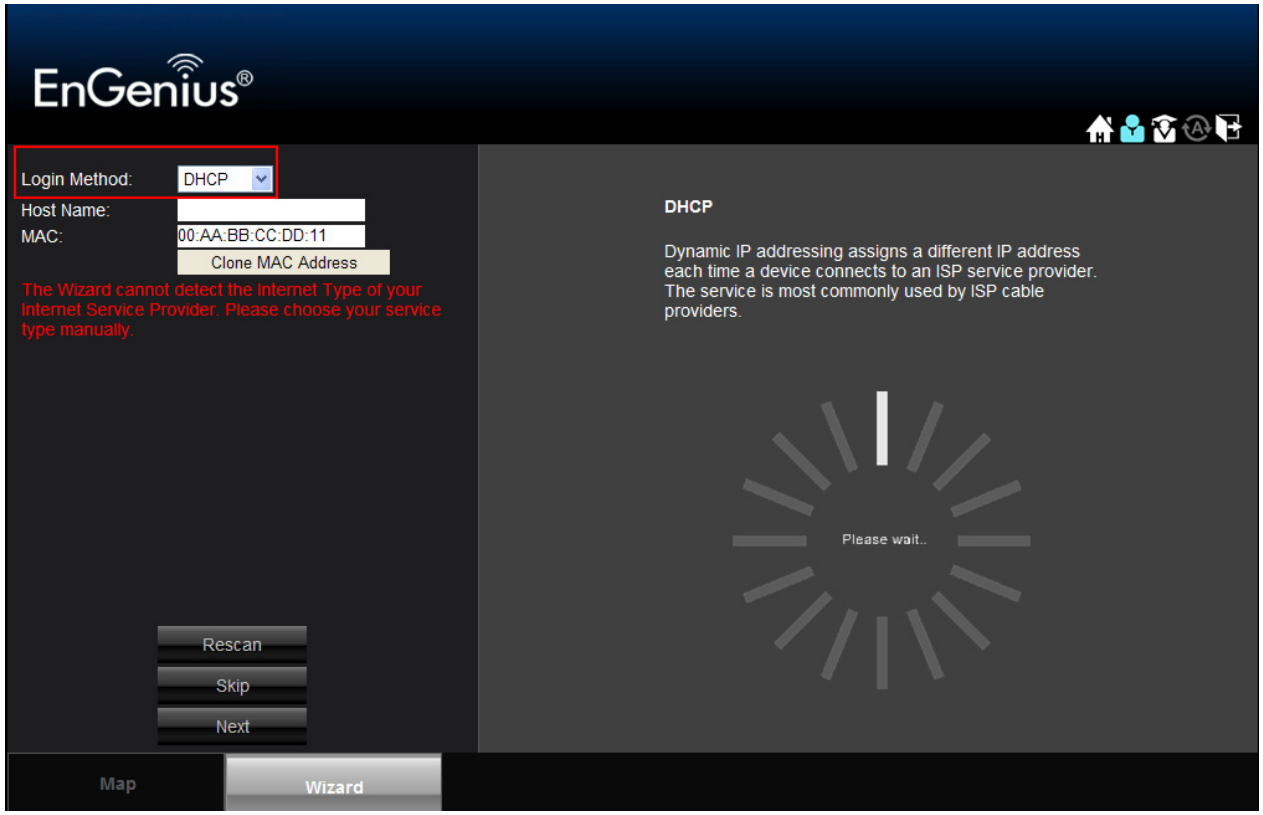
Detecting the Internet Connection in AP Router Mode

1. The Wizard displays a progress bar while detecting the type of Internet connection.



Note:
This process may take several seconds.

2. If the ESR9850v2 can not detect the type of Internet connection, the following screen is displayed.


EnGenius®
Login Method:
DHCP
Host Name:
MAC:
00:AA:BB:CC:DD:11
Clone MAC Address
The Wizard cannot detect the Internet Type of your Internet Service Provider. Please choose your service type manually.
DHCP
Dynamic IP addressing assigns a different IP address each time a device connects to an ISP service provider. The service is most commonly used by ISP cable providers.
Please wait..
Rescan
Skip
Next
Map
Wizard

3. Select a login method from the dropdown list.
4. Fill in the required information.

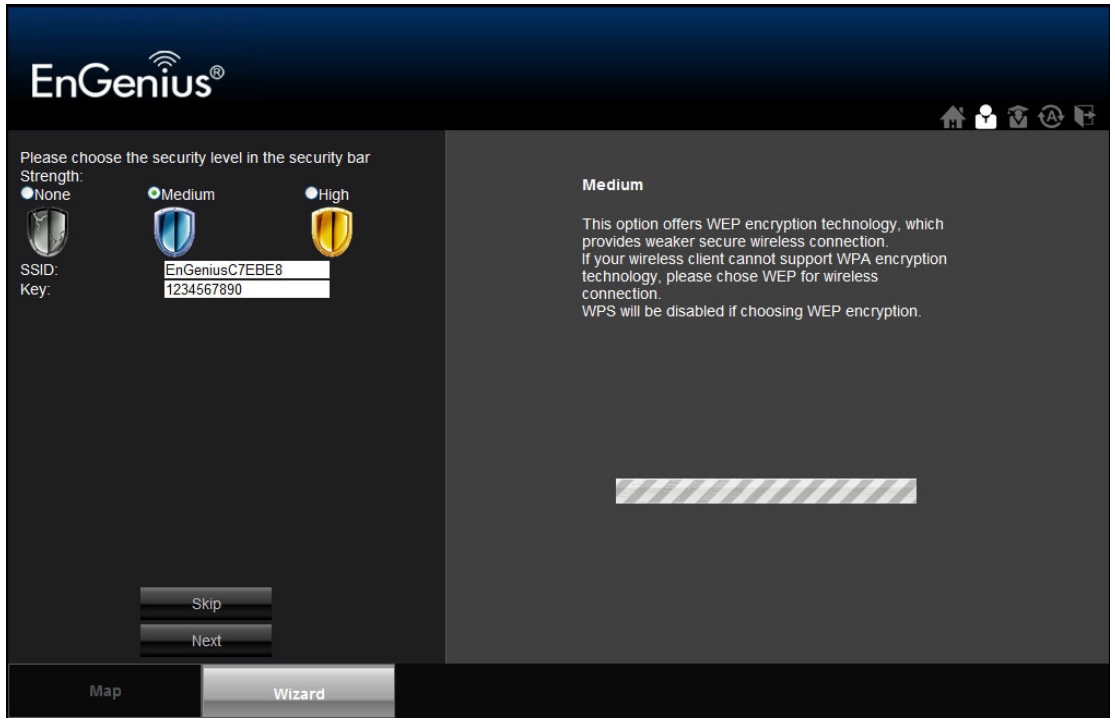
Note:

There are four methods available to connect to the Internet: DHCP, Static IP, PPPoE and LT2P. For a description of each method, refer to “Link Layers” on page 6-85. For configuration instructions, refer to “Configuring Dynamic IP” on page 6-15, “Configuring Static IP” on page 6-17, “Configuring PPPoE” on page 6-18 and “Configuring L2TP” on page 6-22.

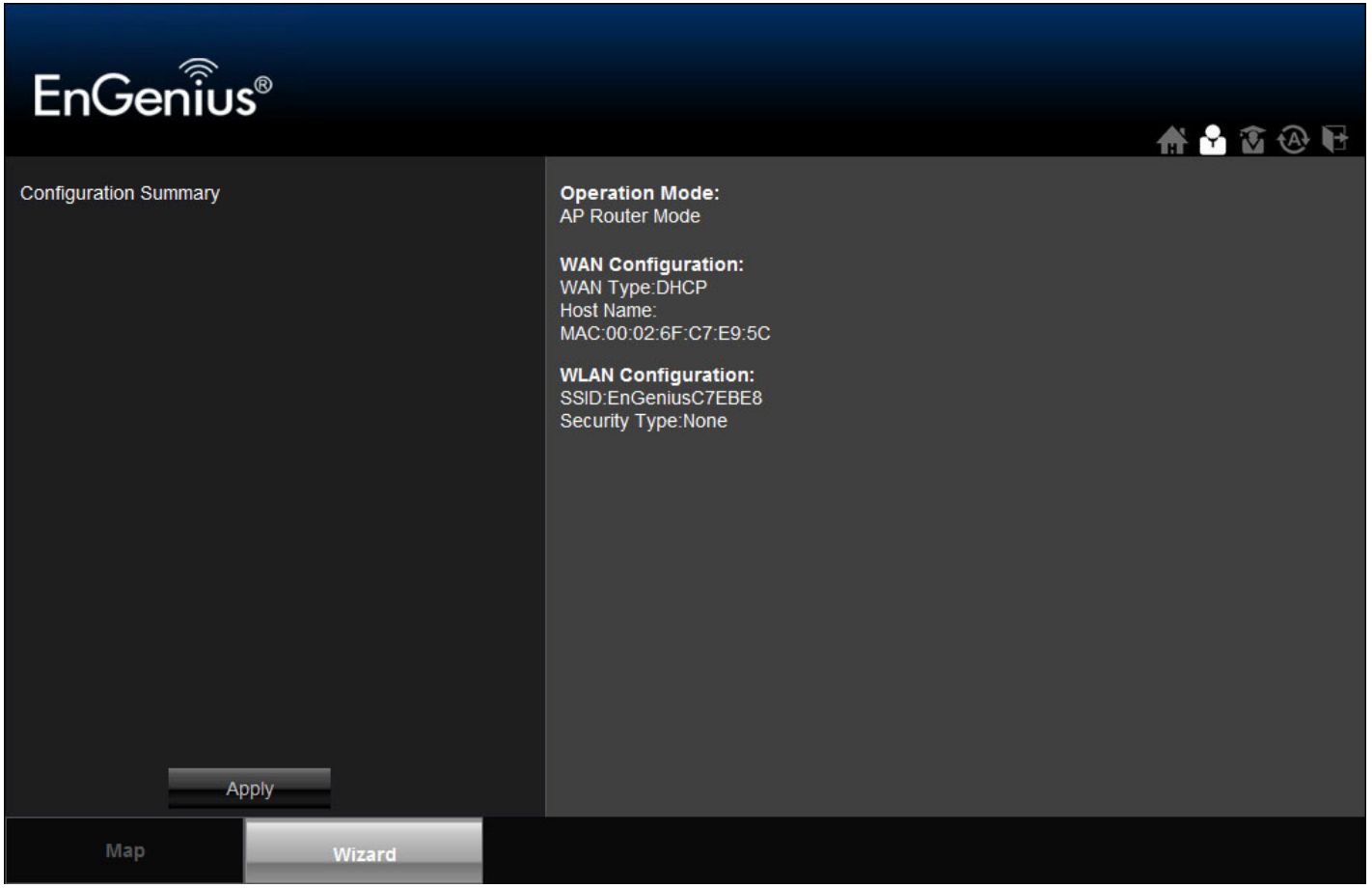
5. Click `Next` to save these settings and continue to the next step; click `Rescan` to detect the Internet connection method; click `Skip` to discard changes and continue to the next step.
6. For the Wireless connection, in the `SSID` text field enter a router name and in the `Key` text field enter a password.

WARNING!

Select High as the security level to best secure the wireless network.



7. Click `Next` to save these settings and continue to the next step or click `Skip` to discard changes and continue to the next step.
8. Review the settings.

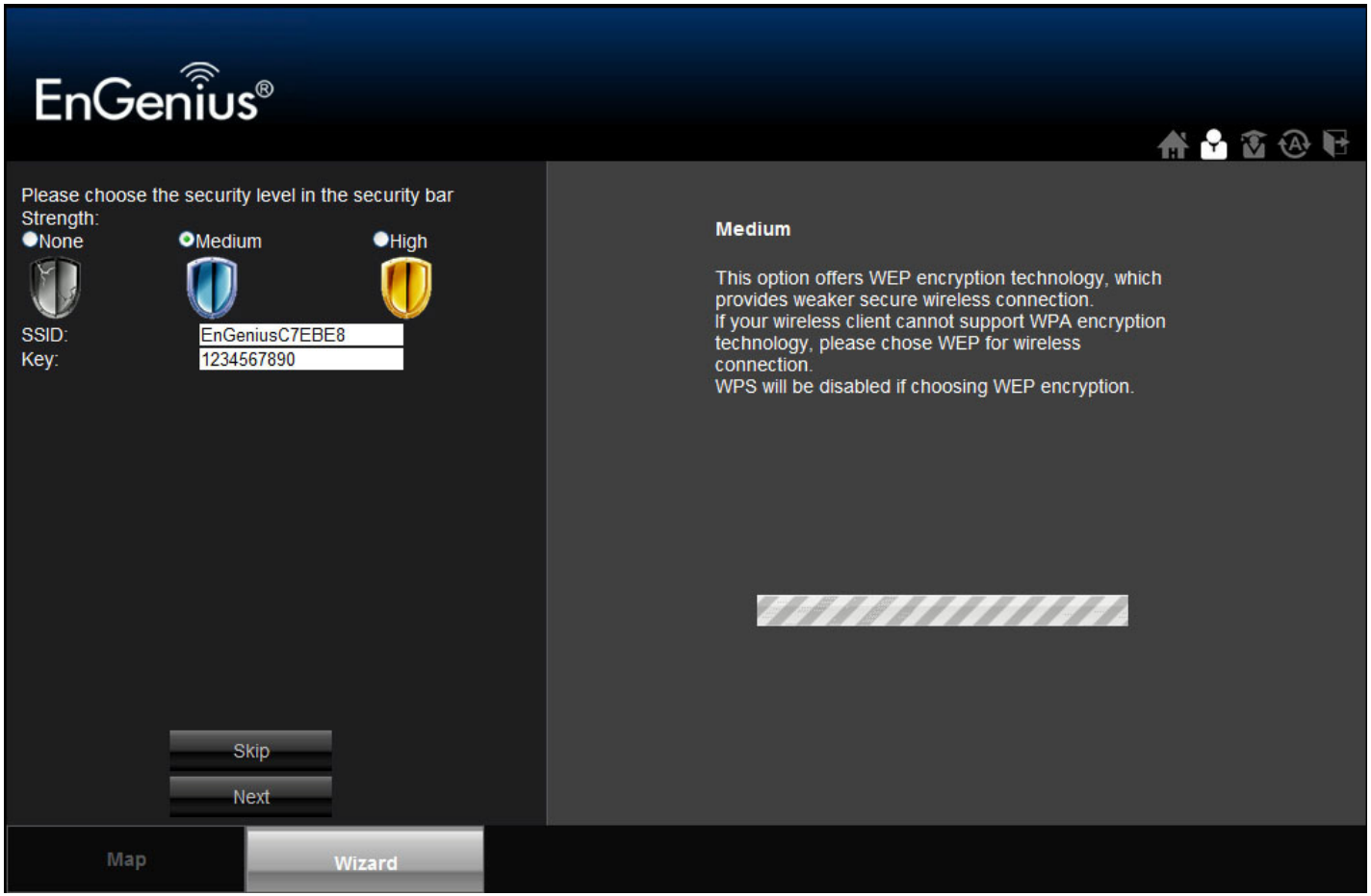


9. Click `Apply` to save the information entered in the previous steps.

The ESR9850v2 setup is complete.

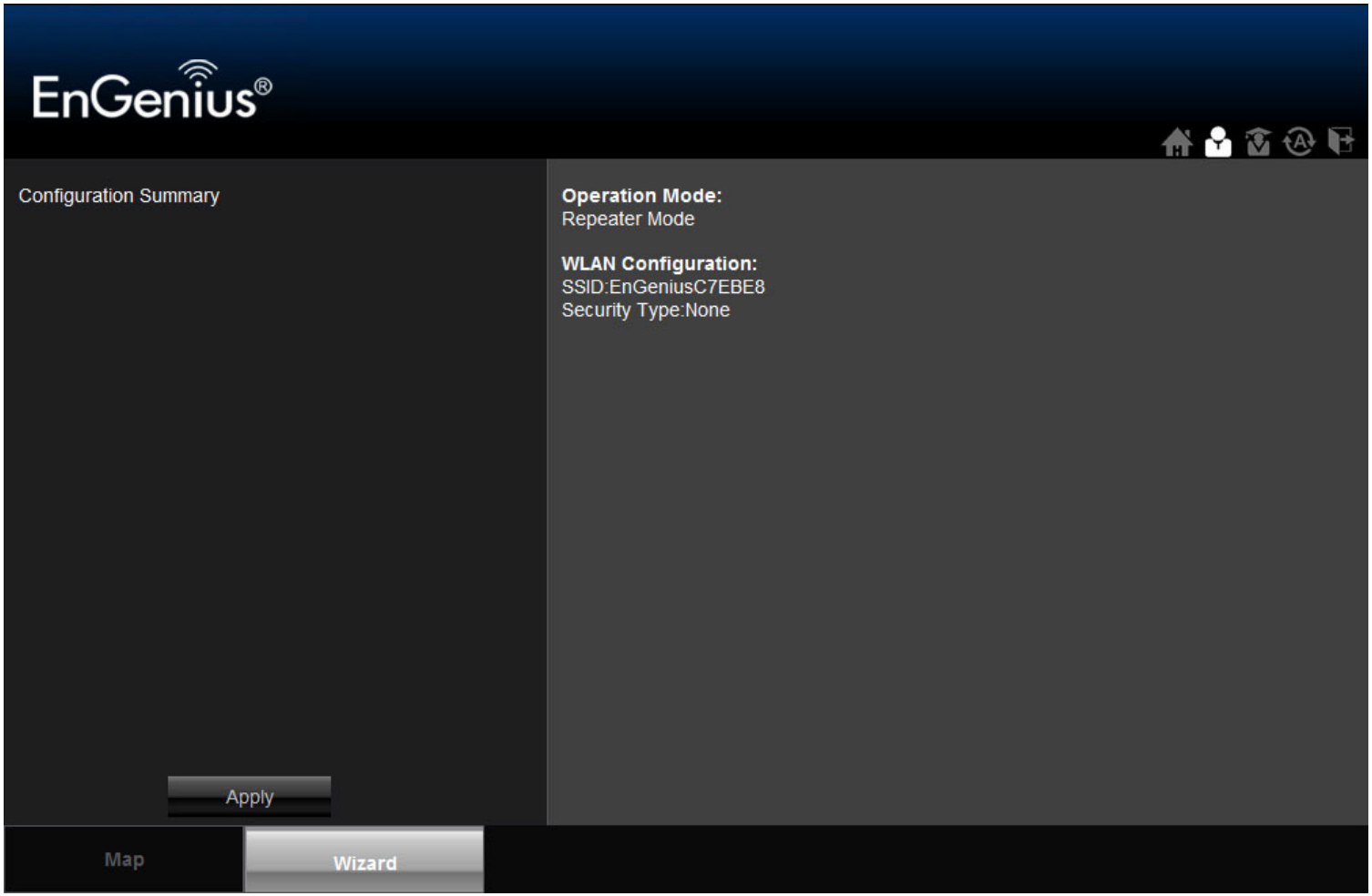
Detecting the Internet Connection in AP Repeater Mode

1. In the `SSID` text field enter a router name and in the `Key` text field enter a password.



2. Click `Next` to save these settings and continue to the next step or click `Skip` to discard changes and continue to the next step.

3. Review the settings.



4. Click `Apply` to save the information entered in the previous steps.

The ESR9850v2 setup is complete.

Basic Network Settings

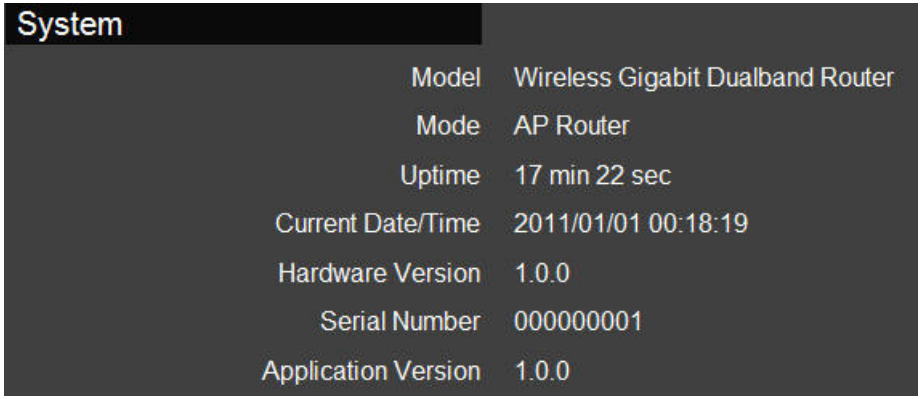
6.2 System Setup

6.2.1 Viewing System Status

The status page shows the summary of the current system status including system (hardware/software version, date/time), Internet connection (WAN), wired network (LAN) and wireless network (WLAN) information.

System

- **Model** The model name of the ESR9850v2.
- **Mode** The router's operating mode (AP Router or WDS).
- **Uptime** The amount of time the device has been active.
- **Current Date/Time** The current system date and time.
- **Hardware Version** The hardware version number of the ESR9850v2.
- **Serial Number** The serial number of the ESR9850v2. The serial number is required for customer service or support.
- **Application Version** The firmware version number of the ESR9850v2.

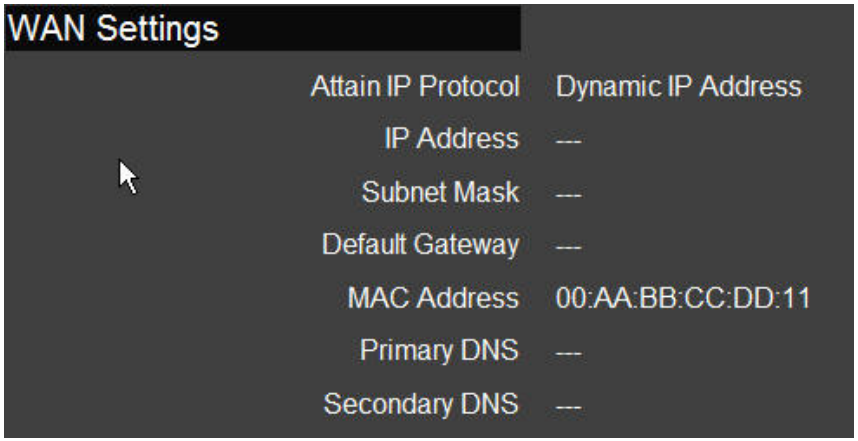


Note:

To update the firmware visit www.engeniusnetworks.com.

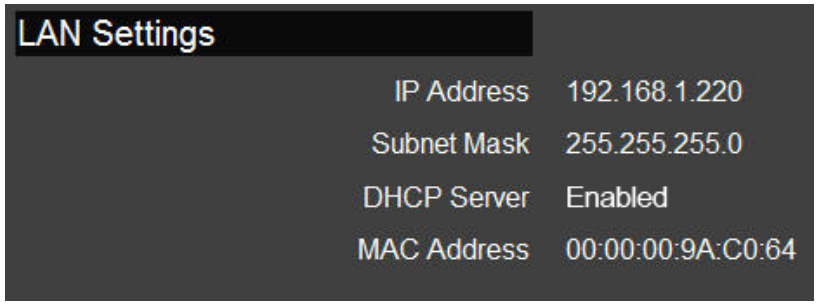
WAN Settings

- **Attain IP Protocol** Displays the IP protocol in use for the ESR9850v2. It can be a dynamic or static IP address.
- **IP Address** The router's IP address as designated by an ISP provider.
- **Subnet Mask** The router's WAN subnet mask as designated by an ISP provider.
- **Default Gateway** The router's gateway address as designated by an ISP provider.
- **MAC Address** The router's WAN MAC address. The router's MAC address is located on the label on the back side of the router.
- **Primary DNS** The primary DNS of an ISP provider.
- **Secondary DNS** The secondary DNS of an ISP provider.



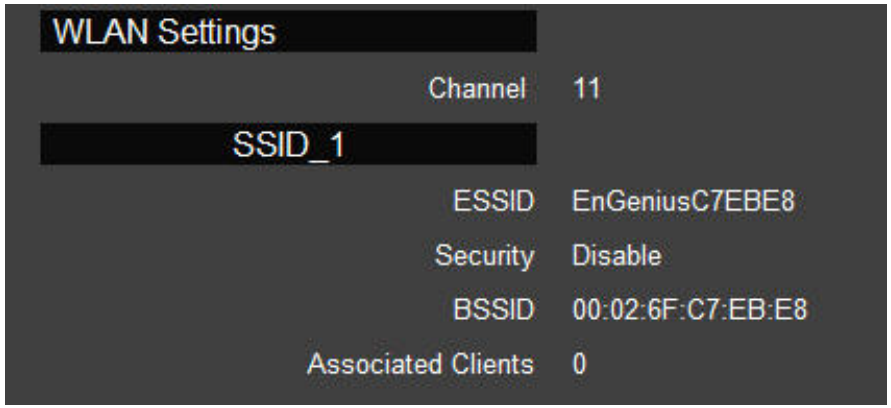
LAN Settings

- **IP Address** The router's local IP address. The default LAN IP address is **192.168.0.1**.
- **Subnet Mask** The router's local subnet mask.
- **DHCP Server:** The DHCP setting status (Default: **Enabled**).
- **MAC Address** The router's LAN MAC address.



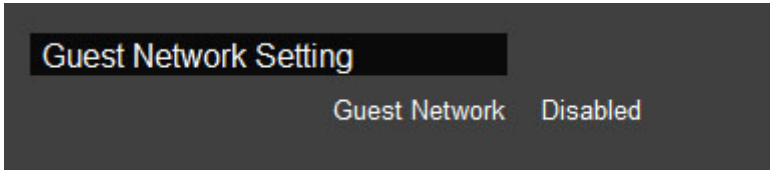
Wireless

- **Channel** The communications channel used by all stations, or computing devices, on the network.
- **ESSID** The ID value of a set of one or more interconnected basic service sets (BSSs).
- **Security** The security setting status (Default: **Disabled**).
- **BSSID** The unique ID of the BSS using the above channel value on this router. The ID is the MAC address of the BSSs access point.
- **Associated Clients** The number of clients associated with this SSID.



Guest Network

Guest Network The guest network status. (Default: **Disabled**)



6.2.1 Configuring Operation Mode

The ESR9850v2 supports two different operation modes: Router Mode and Repeater Mode.

Router Mode

In router mode the internal DHCP server allows a number of LANs to automatically generate IP addresses to share the same Internet connection. In this mode, connect an AP/WISP wirelessly and connect to LANs via a wired connection.

Repeater Mode

Repeater mode is used to regenerate or replicate signals that are weakened or distorted by transmission over long distances and through areas with high levels of electromagnetic interference (EMI).

Note:
The device DHCP server is disabled when the device is set to repeater mode.

Operation Mode Select `AP Router Mode` or `Repeater Mode`.

Note:
The device must restart after changing modes.

6.2.1 Configuring LAN

Configure the wired network settings in the LAN section. The router's IP is defined in the `IP Address` field. The default setting of the DHCP server is set to enabled so that network clients can be automatically assigned a virtual IP addresses. Advanced users may configure DNS server settings to meet specific requirements. Changing the settings in this section are not necessary for most situations.

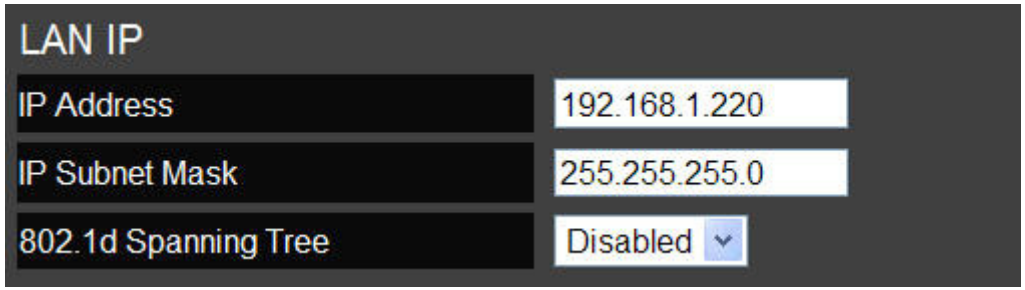
Note:
Keep the default values if you are uncertain of the settings values.

LAN IP

IP Address Configure the router's LAN IP address.

IP Subnet Mask Configure the router's LAN Subnet Mask

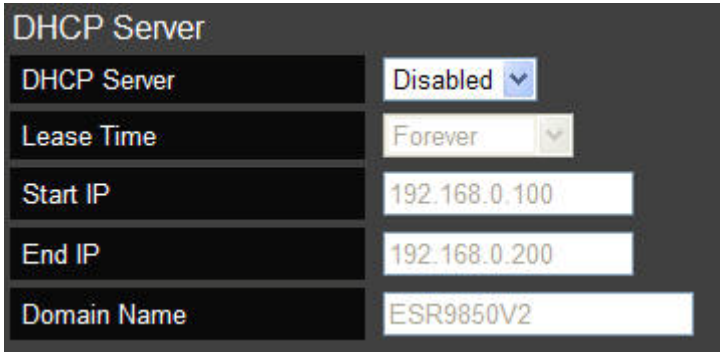
802.1d Spanning Tree The 802.1d Spanning Tree settings is disabled by default. When enabled, the spanning tree protocol is applied to prevent network loops (transmissions won't pass the same node twice to reach the destination).



Note:
The default device IP address is `192.168.0.1`.

DHCP Server

The DHCP server assigns IP addresses to the devices on the LAN.



DHCP Server Enable or disable the DHCP server (Default: **Enabled**).

Lease Time Configure the amount of time each allocated IP address can by used by a client.

Start IP The first IP address in the range of addresses assigned by the router.

End IP The last IP address in the range of addresses assigned by the router.

Domain Name: The domain name of the router.

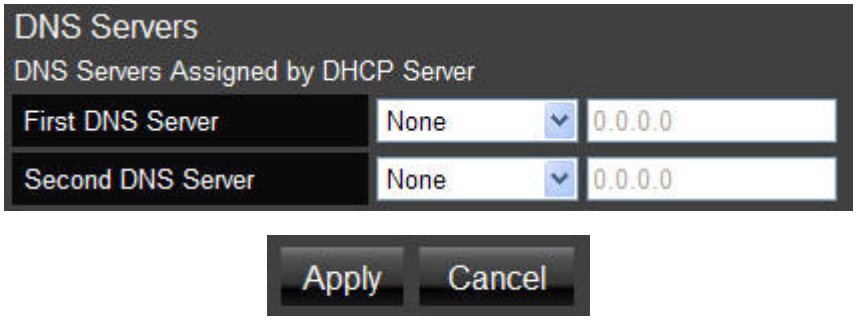
DNS Server

The domain name system (DNS) server translates a domain or website name into a uniform resource locator (URL), or Internet address. There are four options to choose from: From ISP, User-Defined, DNS Relay or None. Select `From ISP` to retrieve the DNS address value from the ISP; select `User-Defined` to assign a custom DNS server address; select DNS Relay to forward all queries to a relay, which in turn sends them to an ISP's DNS server; select `None` to assign no server.

First DNS Server Configure the first, or primary, DNS server. (Default = **None**)

Second DNS Server Configure the second, or secondary, DNS server. (Default = **None**)

Click `Apply` to save the settings.



6.2.1 Configuring DHCP

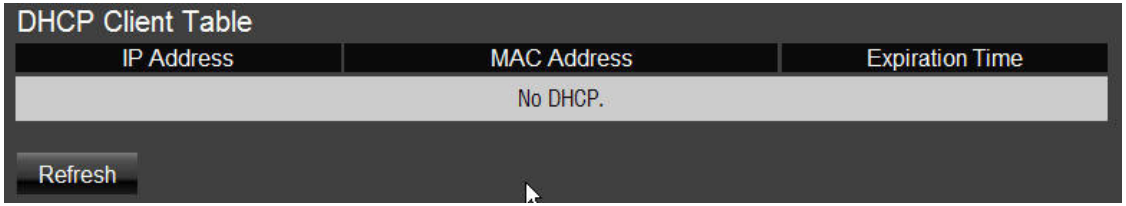
View active dynamically allocated IP (DHCP) addresses and configure and view static DHCP IP addresses.

WARNING!
Do not modify the settings in this section without a thorough understanding of the parameters.

DHCP Client Table

Displays the connected DHCP clients whose IP addresses are assigned by the DHCP server on the LAN.

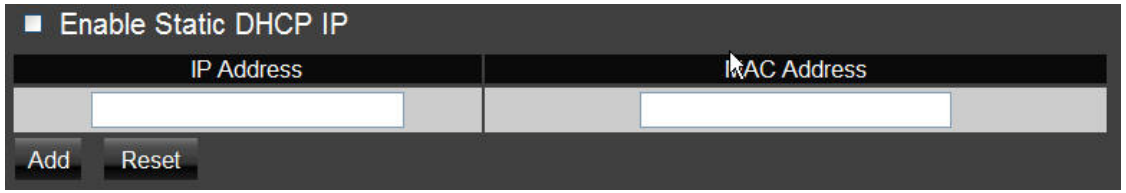
Click `Refresh` to update the table.



Enable Static DHCP IP

Click `Enable Static DHCP IP` to add more static DHCP IP addresses.

Click `Reset` to return the table to its previous state.



Current Static DHCP Table

Active static DHCP addresses are listed along with the associated MAC addresses.

Click `Delete Selected` to remove a selected address. Click `Delete All` to remove all addresses from the table. Click `Reset` to return the table to its previous state.

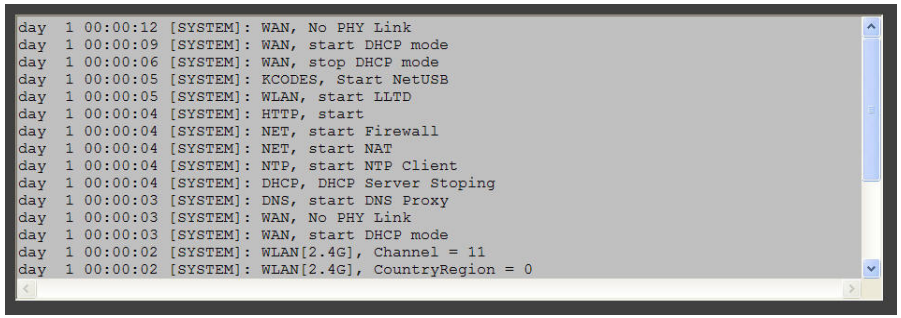
Click `Apply` to save the settings.

6.2.1 Configuring Logging

The logging service records and displays important system information and activity on the network. The events are stored in a memory buffer with older data overwritten by newer when the buffer is full.

Log Message List

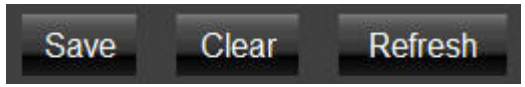
Shows the current system operations and network activity.


day 1 00:00:12 [SYSTEM]: WAN, No PHY Link
day 1 00:00:09 [SYSTEM]: WAN, start DHCP mode
day 1 00:00:06 [SYSTEM]: WAN, stop DHCP mode
day 1 00:00:05 [SYSTEM]: KCODES, Start NetUSB
day 1 00:00:05 [SYSTEM]: WLAN, start LLTD
day 1 00:00:04 [SYSTEM]: HTTP, start
day 1 00:00:04 [SYSTEM]: NET, start Firewall
day 1 00:00:04 [SYSTEM]: NET, start NAT
day 1 00:00:04 [SYSTEM]: NTP, start NTP Client
day 1 00:00:04 [SYSTEM]: DHCP, DHCP Server Stoping
day 1 00:00:03 [SYSTEM]: DNS, start DNS Proxy
day 1 00:00:03 [SYSTEM]: WAN, No PHY Link
day 1 00:00:03 [SYSTEM]: WAN, start DHCP mode
day 1 00:00:02 [SYSTEM]: WLAN[2.4G], Channel = 11
day 1 00:00:02 [SYSTEM]: WLAN[2.4G], CountryRegion = 0

Click `Save` to store data to a log file.

Click `Clear` to empty the log file.

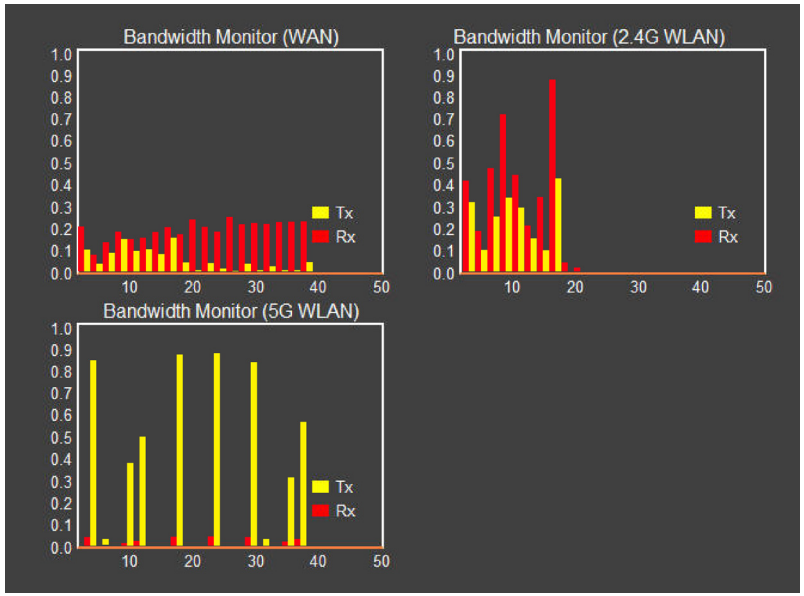
Click `Refresh` to empty the log file and begin updating it with new data.



6.2.1 Monitoring Bandwidth Usage

View bandwidth usage for LAN and WLAN traffic.

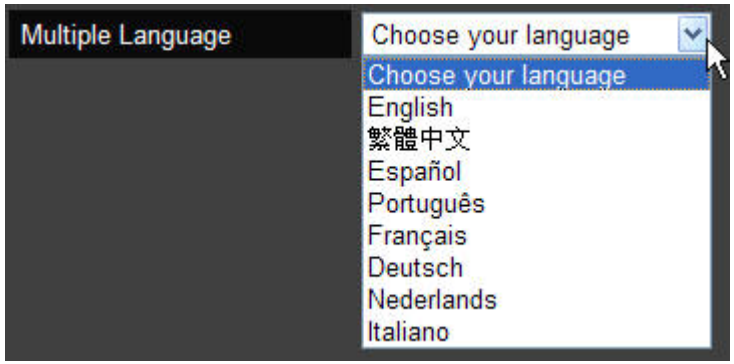
Displays the bandwidth usage for the WLAN and LAN networks.



6.2.1 Configuring Languages

The router supports multiple languages for using the graphical user interface (GUI).

Select the language to use from the dropdown list.



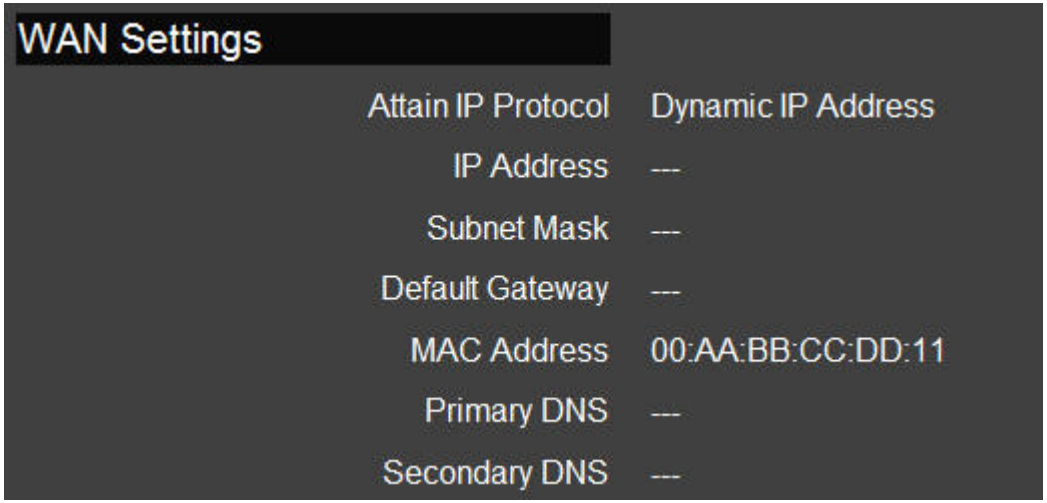
6.3 Configuring WAN Settings

6.3.1 View WAN Status

The WAN Settings, or Internet Status, page shows a summary of the current Internet connection information. This section is also shown on the System Status page.

WAN Settings

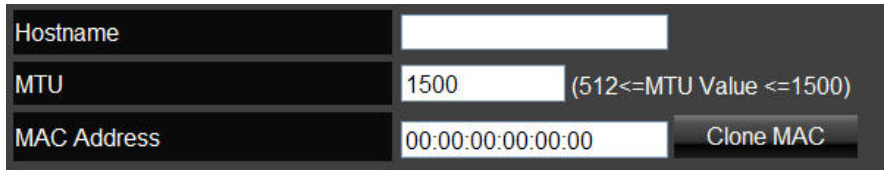
- **Attain IP Protocol** Display the IP Protocol type used for the ESR9850v2 (**Dynamic IP Address** or `Static IP Address`).
- **IP Address** The router's WAN IP address.
- **Subnet Mask** The router's WAN subnet mask.
- **Default Gateway** The ISP's gateway IP address.
- **MAC Address** The router's WAN MAC address. The router's MAC address is located on the label on the back side of the router.
- **Primary DNS** The primary DNS address of an ISP provider.
- **Secondary DNS:** The secondary DNS address of an ISP provider.



6.3.1 Configuring Dynamic IP

Dynamic IP addressing assigns a different IP address each time a device connects to an ISP service provider. The service is most commonly used by ISP cable providers.

Dynamic IP



- **Host name** Assign a name for the internet connection type. This field can be blank.
- **MTU** Configure the maximum transmission unit (MTU). The MTU specifies the largest packet size permitted for an internet transmission. The factory default MTU size for Dynamic IP (DHCP) is 1500. The MTU size can be set between 512 and 1500.
- **Clone MAC** Enter the MAC address of the devices' network interface card (NIC) in the MAC address field and click `Clone MAC`.

Note:

Some ISP providers require registering the MAC address of the network interface card (NIC) connected directly to the cable or DSL modem. Clone MAC masks the router's MAC address with the MAC address of the device's NIC.

DNS Servers

The DNS server translates a domain or website name into a uniform resource locator (URL), or Internet address. There are two options to choose from: From ISP or User-Defined. Select `From ISP` to retrieve the DNS address value from the ISP; select `User-Defined` to assign a custom DNS server address.

- **DNS Server** Configure the type of DNS server. (Default = **From ISP**)
- **First DNS Server** Configure the first, or primary, DNS server.
- **Second DNS Server:** Configure the second, or secondary, DNS server.

Click `Apply` to save the settings or `Cancel` to discard the changes.

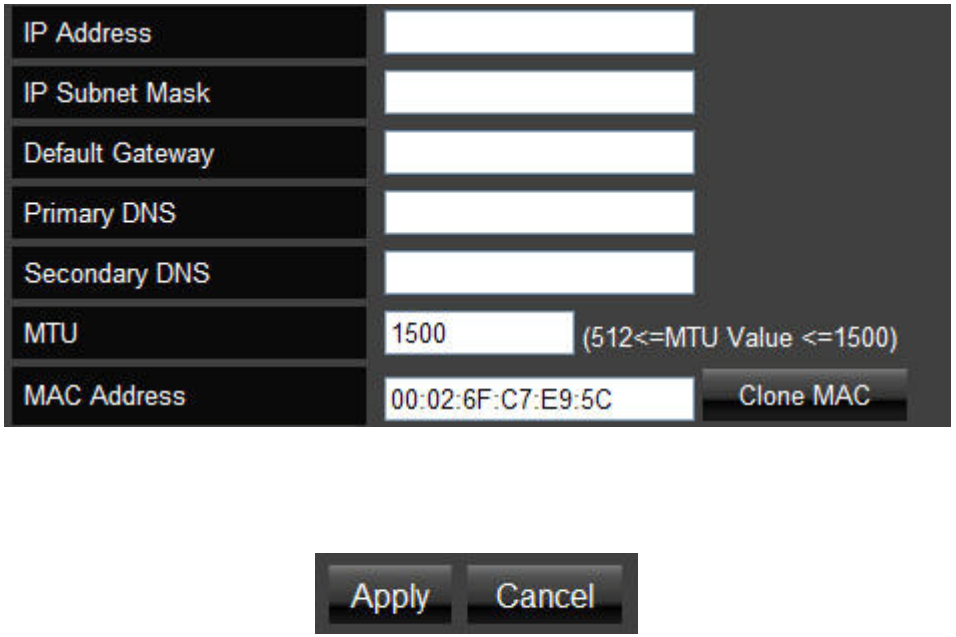
6.3.1 Configuring Static IP

Setting a static IP address allows an administrator to set a specific IP address for the router and guarantees that it can not be assigned a different address.

Static IP

- **IP Address** The router's WAN IP address.
- **Subnet Mask** The router's WAN subnet mask.
- **Default Gateway** The WAN gateway address.
- **Primary DNS** The primary DNS server address.
- **Secondary DNS** The secondary DNS server address.
- **MTU** The maximum transmission unit (MTU) specifies the largest packet size permitted for an internet transmission. The factory default MTU size for static IP is 1500. The MTU size can be set between 512 and 1500.
- **MAC Address** The router's MAC address.

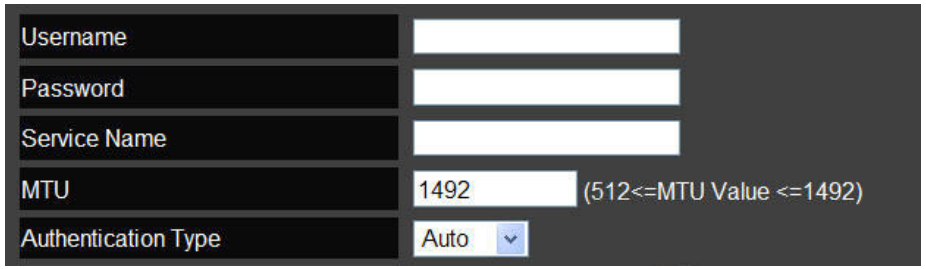
Click `Apply` to save the settings or `Cancel` to discard the changes.



6.3.1 Configuring PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is used mainly by ISPs that provide DSL modems to connect to the Internet.

- **Username** Enter the username assigned by an ISP.
- **Password** Enter the password assigned by an ISP.
- **Service Name** Enter the service name of an ISP (optional).
- **MTU** Enter the maximum transmission unit (MTU). The MTU specifies the largest packet size permitted for an internet transmission (PPPoE default: 1492). The MTU size can be set between 512 and 1492.
- **Authentication Type** Select the type of authentication provided by the ISP: `Auto`, `PAP`, or `CHAP`. If unsure of the best setting, select `Auto` or check with your Internet Service Provider.



- **Type** Configure the connection type between the router and the ISP. Choose between `Keep Connection`, `Automatic Connection` or `Manual Connection`.
- **Idle Timeout** Configure the maximum idle time (1 to 1,000 minutes) allowed for an inactive connection.
- **Clone MAC** Enter the MAC address of the devices' network interface card (NIC) in the MAC address field and click `Clone MAC`.
- Some ISP providers require registering the MAC address of the network interface card (NIC) connected directly to the cable or DSL modem. Clone MAC masks the router's MAC address with the MAC address of the device's NIC.

Click `Apply` to save the settings or `Cancel` to discard the changes.

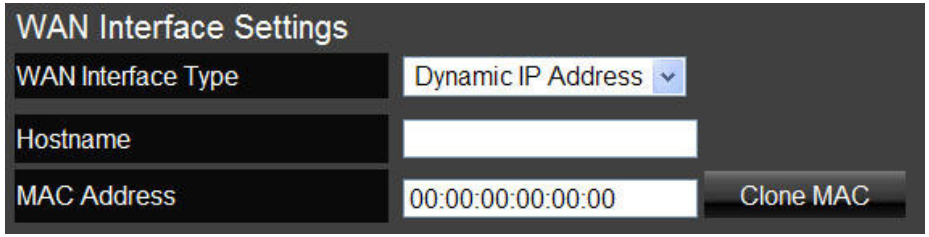
6.3.1 Configuring PPTP

The point-to-point tunnelling protocol (PPTP) is used in association with virtual private networks (VPNs). There a two parts to a PPTP connection: the WAN interface settings and the PPTP settings.

WAN Interface Settings

Dynamic IP Address

- **WAN Interface Type** Select `Dynamic IP Address` to assign an IP address provided by an ISP.
- **Hostname** Enter a host name of an ISP. (optional).
- **Clone MAC** Enter the MAC address of the devices' network interface card (NIC) in the MAC address field and click `Clone MAC`.

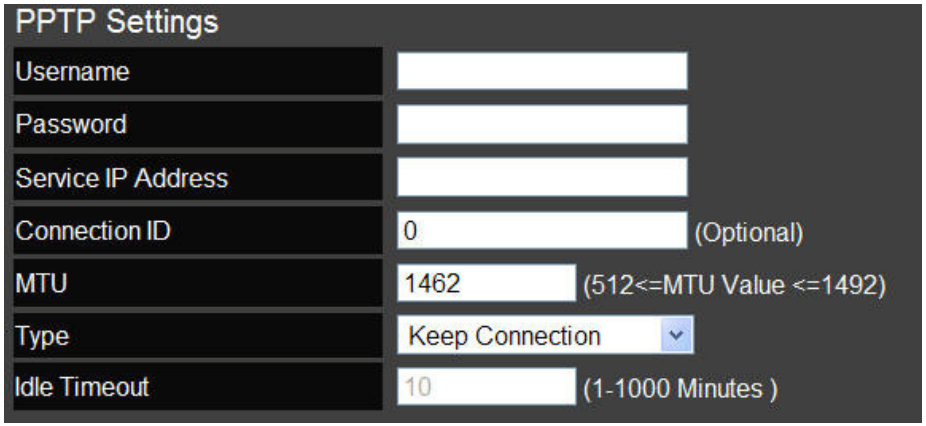


Note:

Some ISP providers require registering the MAC address of the network interface card (NIC) connected directly to the cable or DSL modem. Clone MAC masks the router's MAC address with the MAC address of the device's NIC.

PPTP Settings

- **User Name** Enter the username assigned by your ISP.
- **Password:** Enter the password assigned by your ISP.
- **Service IP Address:** Enter the PPTP server IP address provided by your ISP.
- **Connection ID:** Enter the connection ID provided by your ISP (optional).
- **MTU** Enter the maximum transmission unit (MTU). The MTU specifies the largest packet size (Default: 1462) permitted for an internet transmission. The MTU size can be set between 512 and 1492.
- **Type** Configure the connection type between the router and the ISP. Choose between `Keep Connection`, `Automatic Connection` or `Manual Connection`.
- **Idle Timeout** Configure the maximum amount of time, in minutes, allowed for inactive Internet connection. The Internet connection will be dropped when the maximum idle time is reached. Valid values are between one and one thousand.



Click `Apply` to save the settings or `Cancel` to discard the changes.

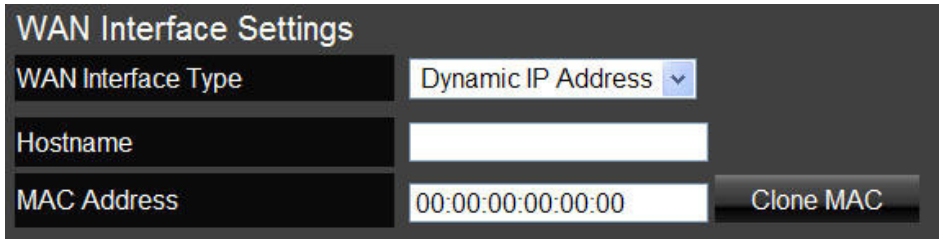
6.3.1 Configuring L2TP

The layer 2 tunneling protocol (L2TP) is used in association with virtual private networks (VPNs). There a two parts to a L2TP connection: the WAN interface settings and the L2TP settings.

WAN Interface Settings

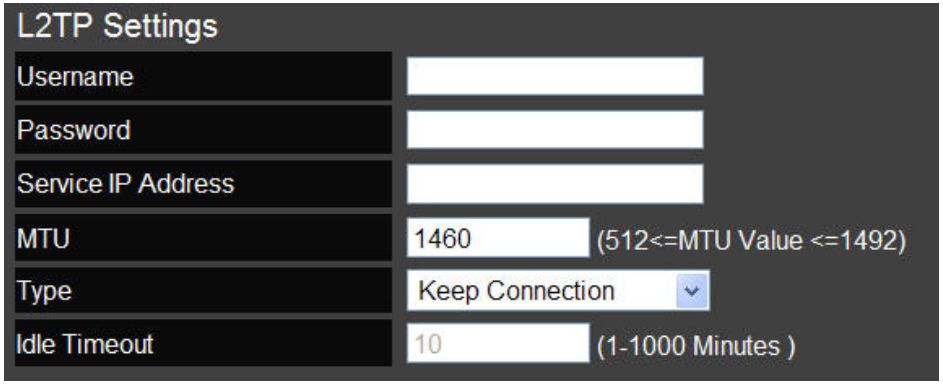
Dynamic IP Address

- **WAN Interface Type** Select `Dynamic IP Address` to assign an IP address provided by an ISP.
- **Hostname** Enter a host name of an ISP (optional).
- **Clone MAC** Enter the MAC address of the devices' network interface card (NIC) in the MAC address field and click `Clone MAC`.
- Some ISP providers require registering the MAC address of the network interface card (NIC) connected directly to the cable or DSL modem. Clone MAC masks the router's MAC address with the MAC address of the device's NIC.



L2TP Settings

- **User Name** Enter the username assigned by an ISP.
- **Password:** Enter the password assigned by an ISP.
- **Service IP Address:** Enter the L2TP server IP address provided by an ISP.
- **Connection ID:** Enter the connection ID provided by an ISP (optional).
- **MTU** Enter the maximum transmission unit (MTU). The MTU specifies the largest packet size (Default: 1460) permitted for an internet transmission. The MTU size can be set between 512 and 1492.
- **Type** Configure the connection type between the router and the ISP. Choose between `Keep Connection`, `Automatic Connection` or `Manual Connection`.
- **Idle Timeout** Configure the maximum amount of time, in minutes, allowed for inactive Internet connection. The Internet connection will be dropped when the maximum idle time is reached. Valid values are between one and one thousand.

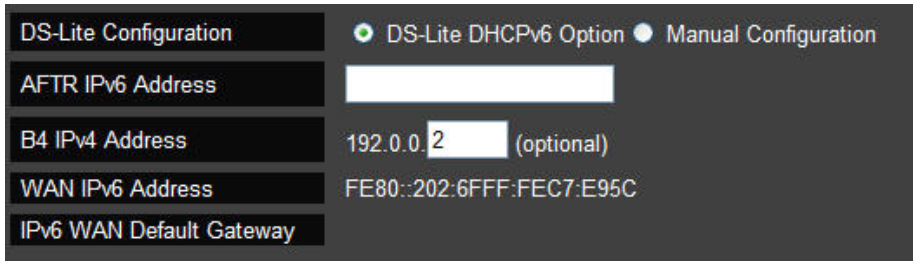


Click `Apply` to save the settings or `Cancel` to discard the changes.

6.3.1 Configuring DS-Lite

Dual-Stack Lite, or DS-Lite, allows ISPs to stop IPv4 addresses from reaching a customer's network devices and only use IPv6.

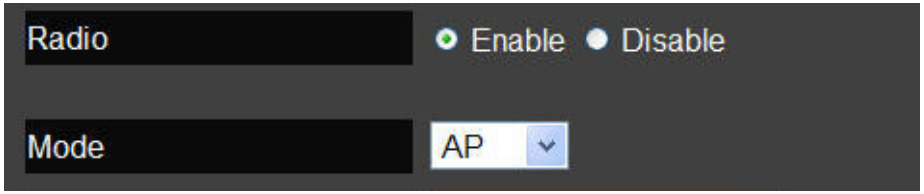
- **DS-Lite Configuration** Select `DS-Lite DHCPv6 Option` or `Manual Configuration`
- **AFTR IPv6 Address** Enter the AFTR IPv6 connection type
- **B4 IPv4 Address** Enter an Optional B4 IPv4 address.
- **WAN IPv6 Address** Enter the WAN IPv6 address.
- **IPv6 WAN Default Gateway** Enter the IPv6 WAN default gateway address.



6.4 Wireless LAN Setup

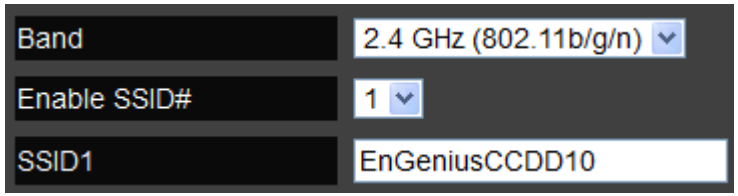
6.4.1 Configuring Basic Settings

- **Radio** Enable or disable the wireless radio. If the wireless radio is disabled, wireless access points are not available.
- **Mode** Select the wireless operating mode for the router. Two modes are available: Access Point or Wireless Distribution System (WDS) mode.
  - **AP** Provides a connection access point for wireless devices.
  - **WDS** Allows the wireless network to be expanded using multiple access points without wired connections.

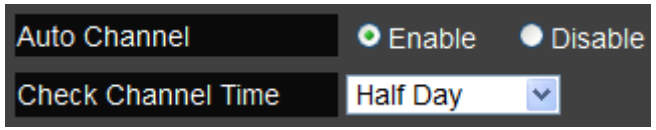


Access Point Mode

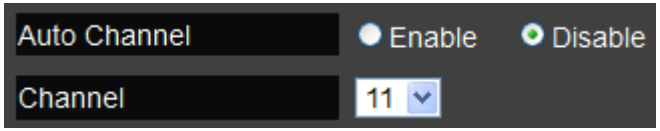
Configure the wireless settings of the router in access point mode.



- **Band:** Select a wireless standard for the network from the following options:
- 2.4 GHz (B)
- 2.4 GHz (N)
- 2.4 GHz (B+G)
- 2.4 GHz (G)
- 2.4 GHz (B+G+N)
- **Enable SSID#** Select the number of wireless groups, between one and four, available on the network.
- **SSID[#]** Enter the name of the wireless network(s).



- **Auto Channel** Enable or disable having the router automatically select a channel for the wireless network. Auto channel is enabled by default. Select disable to manually assign a specific channel. (Default = **Disable**)
- **Check Channel Time** When auto channel is enabled, select time period that the system checks the appropriate channel for the router.



- **Channel** When auto channel is disabled, select a channel to assign to the wireless network. Valid value are from one to eleven in the US and one to thirteen in the EU.

Wireless Distribution System Mode

Configure the router's wireless settings in WDS mode.

- **Channel** Select a channel to assign to the wireless network. Valid value are from one to eleven in the US and one to thirteen in the EU.
- **MAC Address [#]** Enter the MAC address(es) for the wireless access point(s) that are part of the WDS.
- **WDS Data Rate** Select the data rate for the WDS.
- **Set Security** Click `Set Security` to display the WDS security settings screen. For security configuration settings, refer to "WDS Security Settings Screen" on page 6-28.

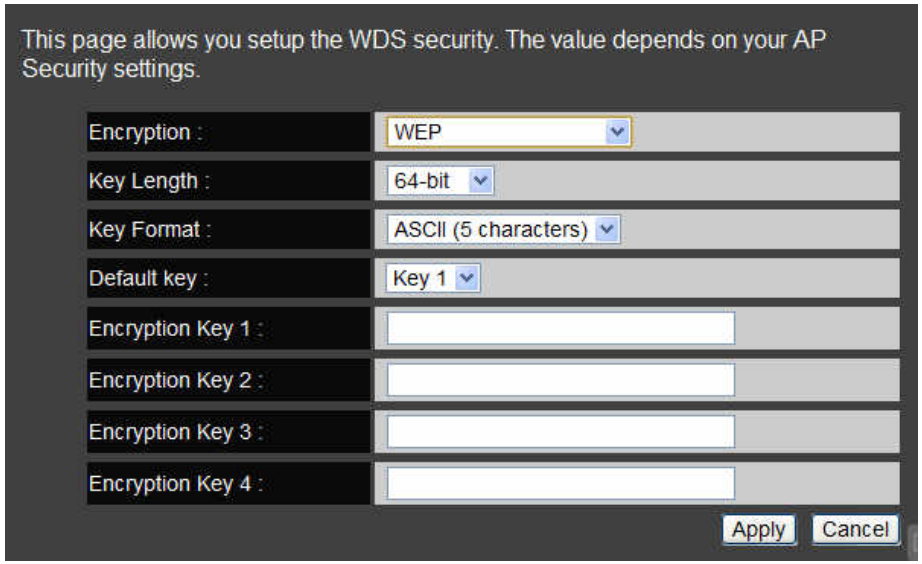
Click `Apply` to save the settings or `Cancel` to discard changes.

WDS Security Settings Screen

Select the type of WDS encryption (`Disable`, `WEP` or `WPA Pre-Shared Key`) for the wireless network.

Wired Equivalent Privacy (WEP)

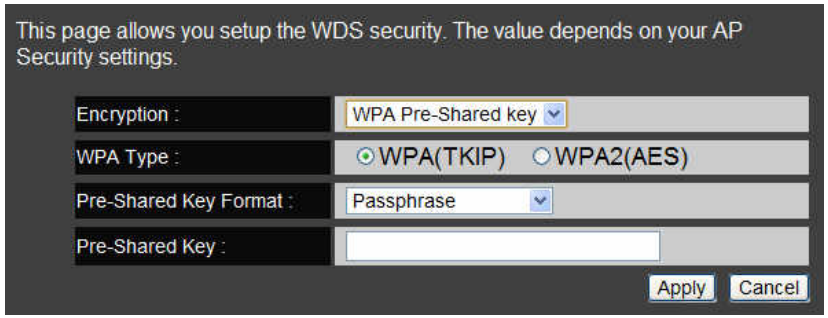
- **Key Length** Select between 64-bit and 128-encryption.
- **Key Format** Select the type of characters used for the WEP Key: `ASCII (5 characters)` or `Hexadecimal (10 characters)`.
- **Default Key** Select the default encryption key for wireless transactions.
- **Encryption Key [#]** Enter the encryption key(s) used to encrypt the data packets during data transmission.
- Click `Apply` to save the settings or `Cancel` to discard changes.



Wi-Fi Protected Access (WPA) Pre-Shared Key

- **WPA Type** Select the type of WPA.
  - **WPA Temporal Key Integrity Protocol (TKIP)** Generates a 128-bit key for each packet.
  - **WPA2 Advanced Encryption Standard (AES)** Government standard packet encryption which is stronger than TKIP.
- **Pre-Shared Key Type** Select the type of pre-shared key as `Passphrase (ASCII)` or `Hexadecimal`.
- **Pre-Shared Key** Enter the pre-shared Key value.

Click `Apply` to save the settings or `Cancel` to discard changes.

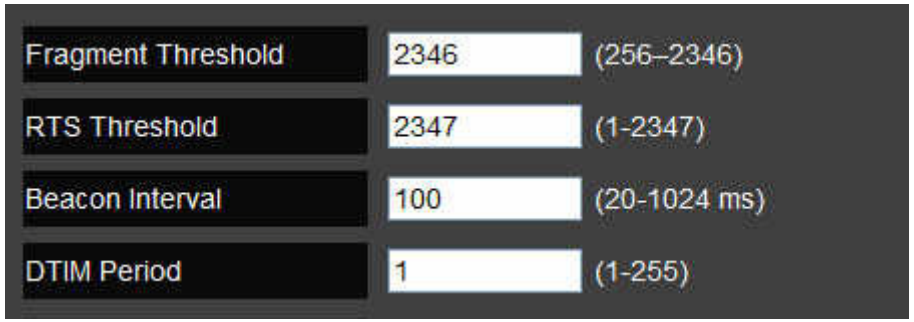


6.4.1 Configuring Advanced Settings

Advanced settings parameters available on the router.

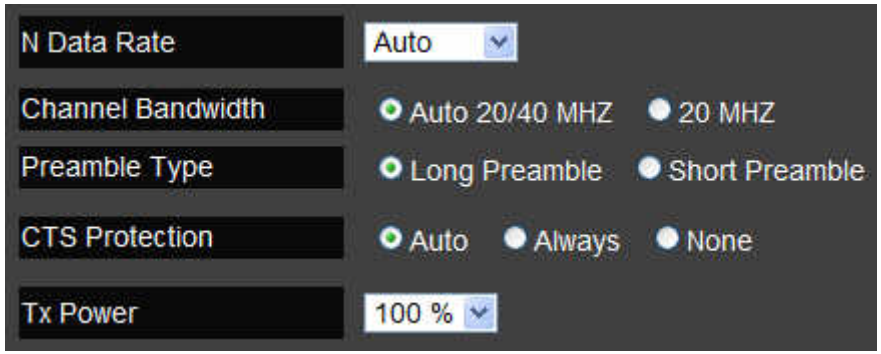
WARNING!
Incorrectly changing these settings may cause the device to stop functioning. Do not modify the settings in this section without a thorough understanding of the parameters.

- **Fragment Threshold** Enter the maximum size of a packet during data transmission. A value too low could lead to low performance.
- **RTS Threshold** Enter the RTS threshold. If the packet size is smaller than the RTS threshold, the ESR9850v2 does not use RTS/CTS to send the data packet.
- **Beacon Interval** Enter the beacon interval. This is the amount of time that the ESR9850v2 sets to synchronize the network.
- **Delivery Traffic Indication Message (DTIM) Period** Enter the DTIM period. The DTIM is a countdown period informing clients of the next point of broadcast and multi-cast of messages over the network. Valid values are between 1 and 255.



- **N Data Rate** Select the N data rate. This is the rate in which the ESR9850v2 will transmit data packets to wireless N compatible devices.
- **Channel Bandwidth** Select the channel bandwidth. The factory default is `Auto 20/40MHz`. The default setting provides the best performance by auto selecting channel bandwidth.
- **Preamble Type** Select the preamble type. `Long Preamble` provides better LAN compatibility and `Short Preamble` provides better wireless performance.
- **CTS Protection** Select the type of CTS protection. Using CTS Protection can lower the data collisions between Wireless B and Wireless G devices and lower data throughput.
- **Tx Power** Select the wireless signal strength level. Valid values are between 10% and 100%.

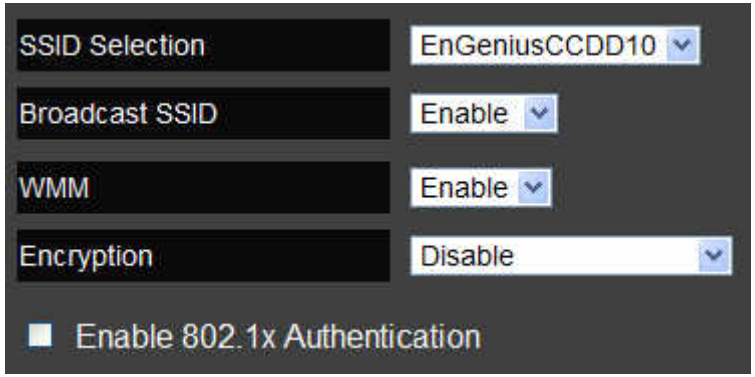
Click `Apply` to save the settings or `Cancel` to discard changes.



6.4.1 Configuring Security

Enable security options on the wireless network to prevent intrusions to systems on the wireless network.

- **SSID Selection** Select the wireless network group to change the wireless security settings for.
- **Broadcast SSID** Enable or disable broadcast SSID. Choose whether or not the wireless group is visible to other members.
- **Wi-Fi Multimedia (WMM)** Enable or disable quality of server (QoS) to optimize the streaming for bandwidth sensitive data such as HDTV video streaming, online gaming, VoIP, videoconferencing, and etc.
- **Encryption** Select the encrypt type for the router.
- **Enable 802.1x Authentication** Enable or disable 802.1x authentication.



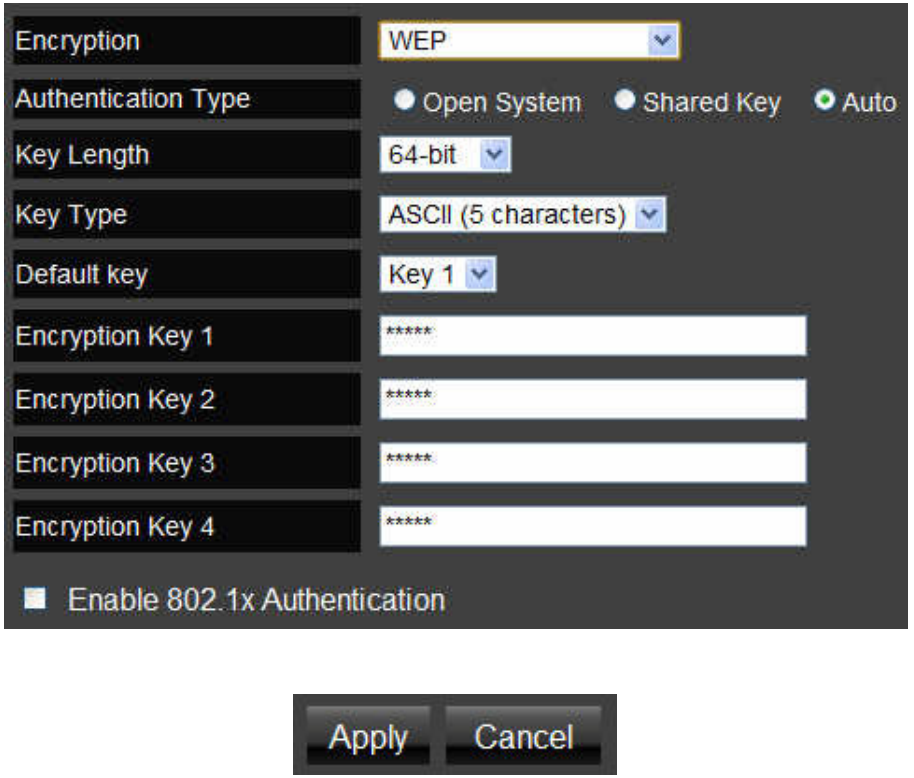
Click `Apply` to save the settings or `Cancel` to discard the changes.

Encryption Type

Wired Equivalent Privacy (WEP)

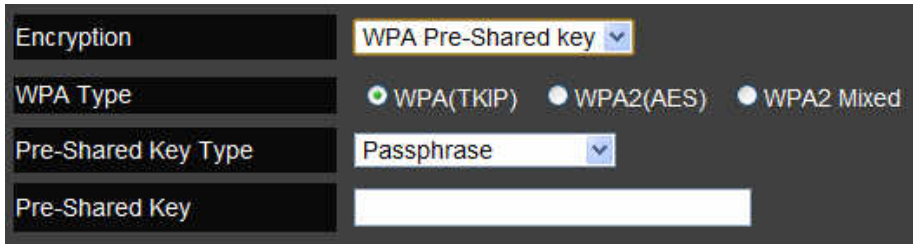
- **Authentication Type** Select the type of authentication.
  - **Open System** Wireless stations can associate with the ESR9850v2 without WEP encryption
  - **Shared Key** Devices must provide the corresponding WEP key(s) when connecting to the ESR9850v2.
  - **Auto**
- **Key Length** Select between 64-bit and 128-encryption.
- **Key Type** Select the type of characters used for the WEP Key: `ASCII (5 characters)` or `Hexadecimal (10 characters)`.
- **Encryption Key [#]** Enter the encryption key(s) used to encrypt the data packets during data transmission.
- **Enable 802.1x Authentication** Enable or disable 802.1x authentication.

Click `Apply` to save the settings or `Cancel` to discard the changes.



Encryption: Wi-Fi Protected Access (WPA) Pre-Shared Key

- **WPA Type** Select the type of WPA.
  - **WPA Temporal Key Integrity Protocol (TKIP)** Generates a 128-bit key for each packet.
  - **WPA2 Advanced Encryption Standard (AES)** Government standard packet encryption which is stronger than TKIP.
  - **WPA2 Mixed** Mixed mode allows device to try WPA2 first, and if that fails selects WPA type.
- **Pre-Shared Key Type** Select the type of pre-shared key as `Passphrase (ASCII)` or `Hexadecimal`.
- **Pre-Shared Key** Enter the pre-shared Key value.

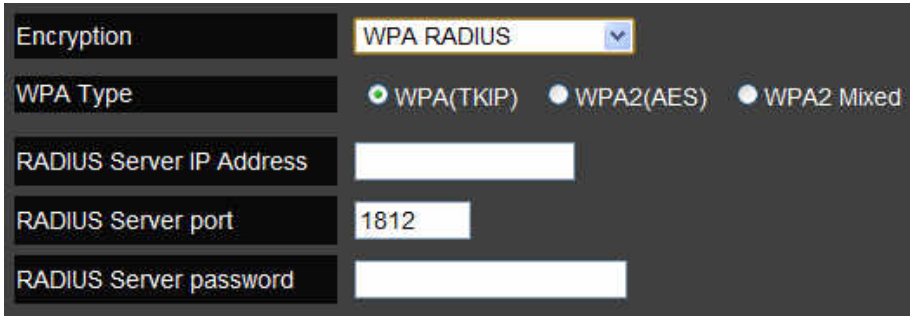


Click `Apply` to save the settings or `Cancel` to discard the changes.

Encryption: WPA RADIUS

Use a RADIUS server to authenticate wireless stations and provide a session key to encrypt data during communications.

- **WPA Type** Select the type of Wireless Protected Access (WPA).
  - **WPA Temporal Key Integrity Protocol (TKIP)** Generates a 128-bit key for each packet.
  - **WPA2 Advanced Encryption Standard (AES)** Protects unauthorized access by verifying network users (encryption is stronger than TKIP).
  - **WPA2 Mixed** Mixed mode allows device to try WPA2 first, and if that fails selects WPA type.
- **RADIUS Server IP Address:** Enter the IP address of the server.
- **RADIUS Server Port**: Enter the port number of the server.
- **RADIUS Server Password:** Enter the password of the server.



Click `Apply` to save the settings or `Cancel` to discard changes.

6.4.1 Configuring Filter

WARNING!
Incorrectly changing these settings may cause the device to stop functioning. Do not modify the settings in this section without a thorough understanding of the parameters.

When `Enable Wireless Access Control` is selected, only wireless clients with MAC addresses listed in the table are allowed to connect to the wireless network.

Enable Wireless Access Control

- **Description** Enter a description of the device allowed to connect to the network.
- **MAC Address** Enter the MAC address of the wireless device.

Click `Add` to append a new device to the list or `Reset` to discard changes.

MAC Address Filtering Table

- **No.** The sequence number of the device.
- **Description** The description of the device.
- **MAC Address** The MAC address of the device.
- **Select** Indicates the device(s) that can have actions performed on them.

Click `Delete Selected` to remove selected devices from the list.

Click `Delete All` to remove all devices form the list.

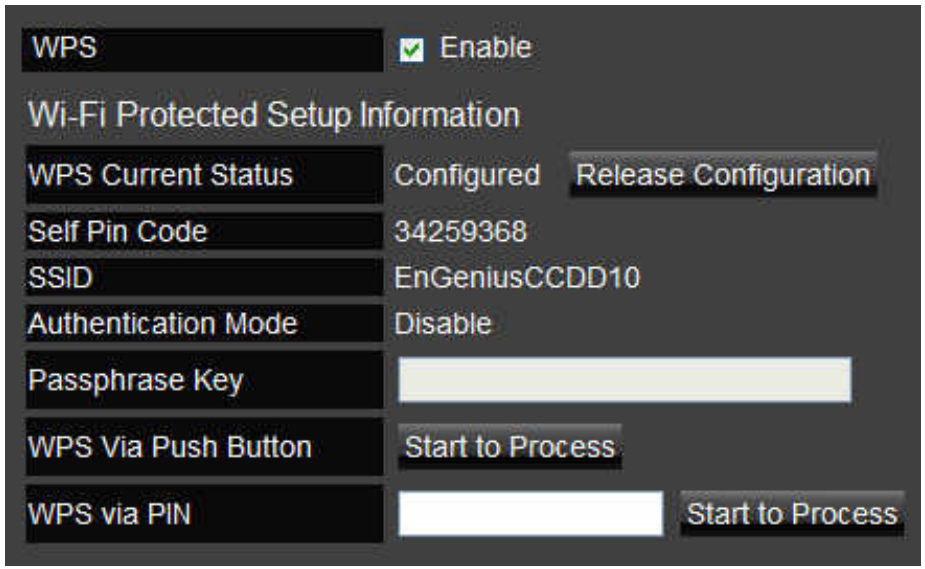
Click `Reset` the discard changes.

Click `Apply` to save the settings or `Cancel` to discard changes.

6.4.1 Configuring Wi-Fi Protected Setup

Wi-Fi protected setup (WPS) is an easy way to allow wireless clients to connect to the ESR9850v2. Automate the connection between the device and the ESR9850v2 using a button or a PIN.

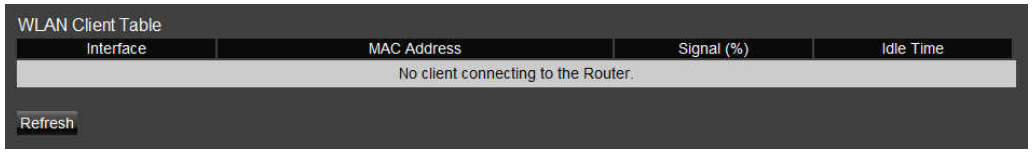
- **WPS** Enable or disable WPS.
- **WPS Current Status** A notification of whether or not wireless security is configured.
- **Self Pin Code** An 8-digit PIN which is required when configuring the router for the first time in Windows 7 or Vista.
- **SSID** The name of the wireless network.
- **Authentication Mode** The current security settings for the corresponding SSID.
- **Passphrase Key** A randomly generated key created by the ESR9850v2 during WPS.
- **WPS via Push Button** Click `Start to Process` to activate WPS.
- **WPS via PIN** Enter the PIN of a wireless device click `Start to Process` to activate WPS.



6.4.1 Configuring Client List

View the wireless devices currently connected to the ESR9850v2.

- **Interface** The type of network connected to the device.
- **MAC Address** The MAC address of device connected to network.
- **Signal** The signal strength of the device connected to the network.
- **Idle Time** The amount of time the connected device has not been active on the network.
- Click `Refresh` to refill the list with currently connected devices.



6.5 Guest Network

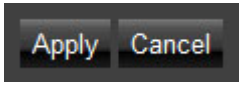
The Guest Network function enables you to offer Internet connectivity to visitors or guests while keeping other networked devices (computers and hard drives) and sensitive personal or company information private and secure.

The Guest Network is controlled by the Wireless SSID function. When the Guest Network function is enabled, the Guest SSID can only get the internet connection from WAN, but can not reach the client from the LAN port.

6.5.1 Enabling Guest Network

- **Guest Network** Enable or Disable the Guest Network function
- **Client Isolation** Guest clients are isolated and can not communicate with each other.
- **SSID** Choose a SSID for the Guest Network used. The SSID can be defined from the Wireless setting page.

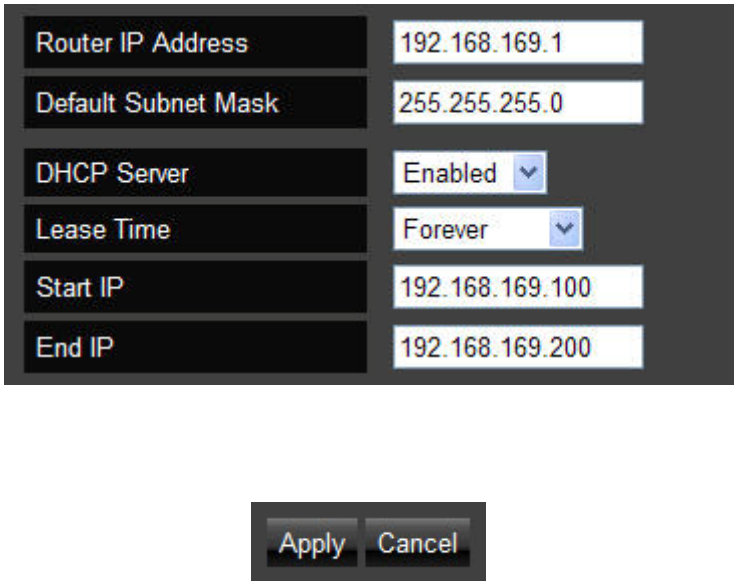
Click `Apply` to save the settings or `Cancel` to discard changes.



6.5.1 Configuring Guest IP Address

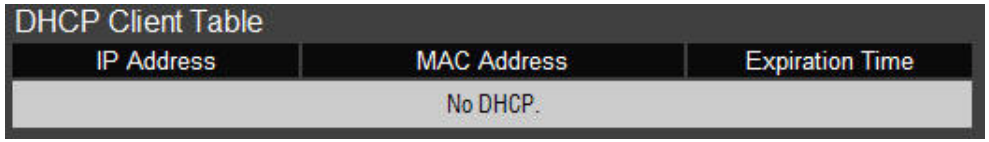
- **Router IP address** Define the router IP address for the Guest network
- **Default Subnet Mask** Define the Subnet Mask IP address for the Guest network
- **DHCP server** To enable or disable the Guest network DHCP server
- **Lease Time** To define the Guest Network DHCP server lease time
- **Start IP** To define the Guest network DHCP server start IP
- **End IP** To define the Guest network DHCP server end IP

Click `Apply` to save the settings or `Cancel` to discard changes.

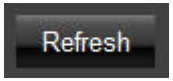


6.5.1 Viewing Guest Client List

DHCP Client Table View the guest network client list.



Click `Refresh` to refresh the view of the list.



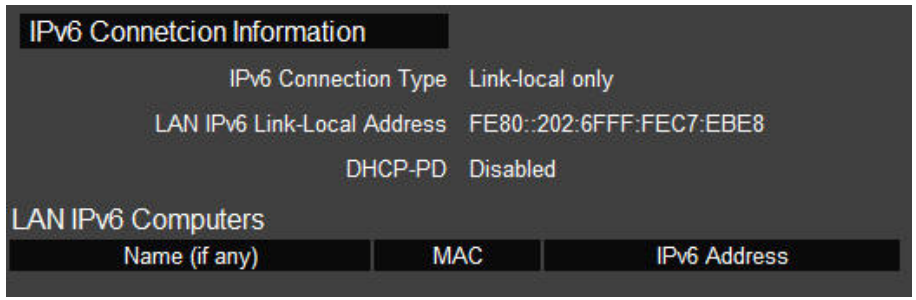
6.6 IPv6

There are several connection types to choose from: Auto Detection, Static IPv6, Autoconfiguration (SLAAC/DHCPv6), PPPoE, IPv6 in IPv4 Tunnel, 6to4, 6rd, and Link-local. If you are unsure of your connection method, please contact your IPv6 Internet Service Provider.

Note:
If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled.

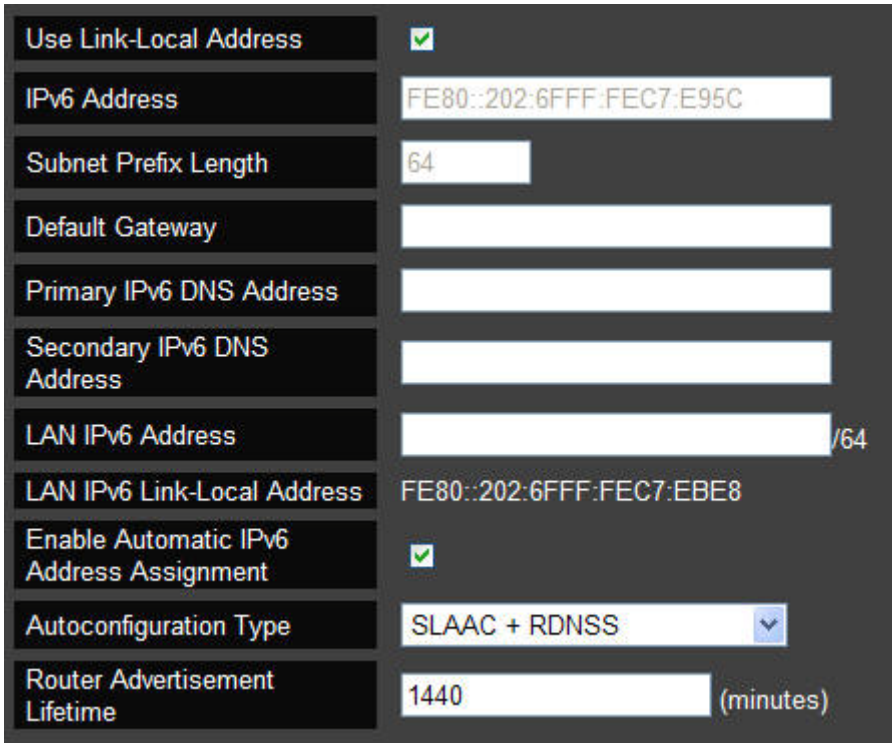
6.6.1 View IPv6 Status

- **IPv6 Connection Information** Shows the IPv6 connection type, the LAN IPv6 link-local address and the DHCP-PD.
- **LAN IPv6 Computers Table** Shows a list of network computers and their IPv6 connection information.

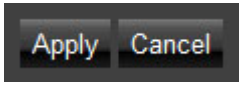


6.6.1 Static IPv6

- **Use Link-Local Address** Enable or disable LAN link-local address.
- **IPv6 Address** Enter the LAN (local) IPv6 address for the router.
- **Subnet Prefix Length** Enter the subnet prefix length.
- **Default Gateway** Enter the default gateway.
- **Primary IPv6 DNS Address** Enter the primary IPv6 DNS address.
- **Secondary IPv6 DNS Address** Enter the secondary IPv6 DNS address.
- **LAN IPv6 Address** Enter the LAN IPv6 address.
- **LAN IPv6 Link-Local Address** Enter the LAN IPv6 link-local address.
- **Enable Automatic IPv6 Address Assignment** Enable or disable automatic IPv6 address assignment.
- **Autoconfiguration Type** Enter the autoconfiguration type. (Default: `SLAAC +RDNSS`).
- **Router Advertisement Lifetime** Enter the IPv6 Address Lifetime (in minutes).

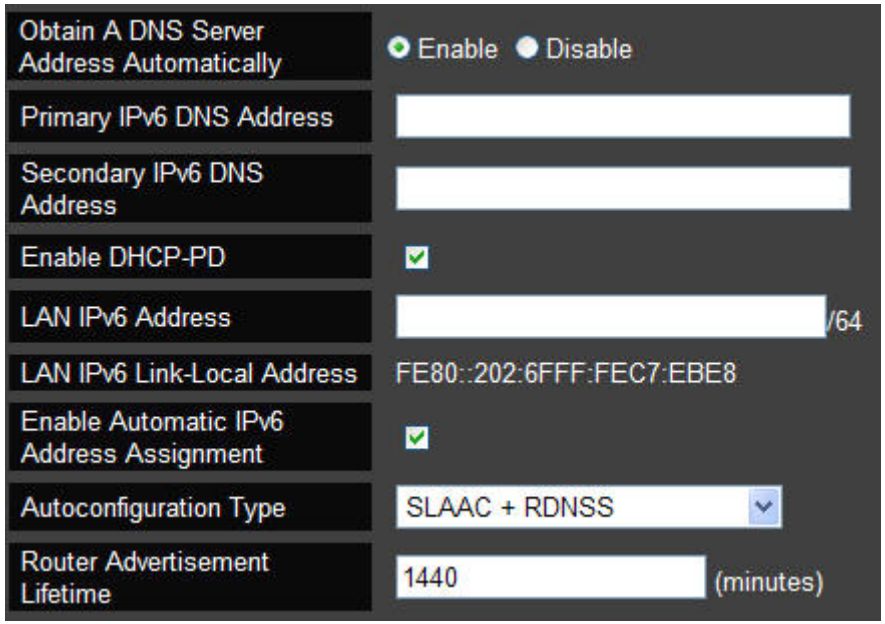


Click `Apply` to save the settings or `Cancel` to discard changes.

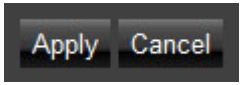


6.6.1 Configure Autoconfiguration

- **Obtain A DNS Server Address Automatically** Enable or disable obtaining a DNS server automatically.
- **Primary IPv6 DNS Address** Enter the primary IPv6 DNS address.
- **Secondary IPv6 DNS Address** Enter the secondary IPv6 DNS address.
- **Enable DHCP-PD** Enable or disable DHCP-prefix delegation (PD).
- **LAN IPv6 Address** Enter the LAN IPv6 address.
- **LAN IPv6 Link-Local Address** Enter the LAN IPv6 link-local address.
- **Enable Automatic IPv6 Address Assignment** Enable or disable automatic IPv6 address assignment.
- **Autoconfiguration Type** Enter the autoconfiguration type. (Default: `SLAAC +RDNSS`)
- **Router Advertisement Lifetime** Enter the IPv6 Address Lifetime (in minutes).

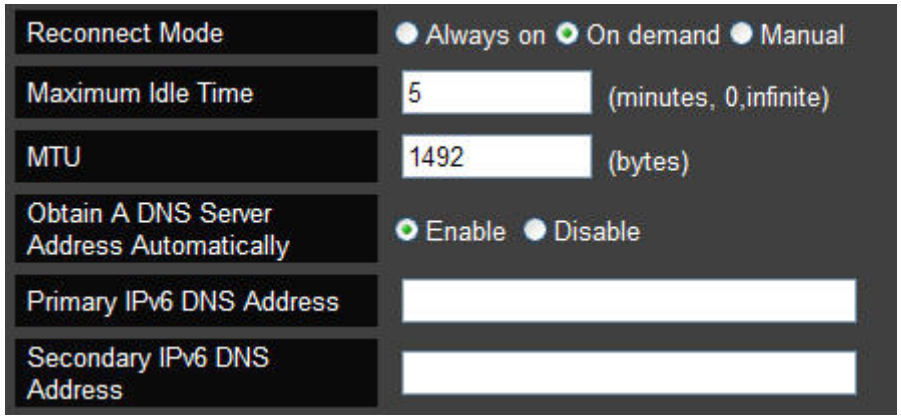


Click `Apply` to save the settings or `Cancel` to discard changes.



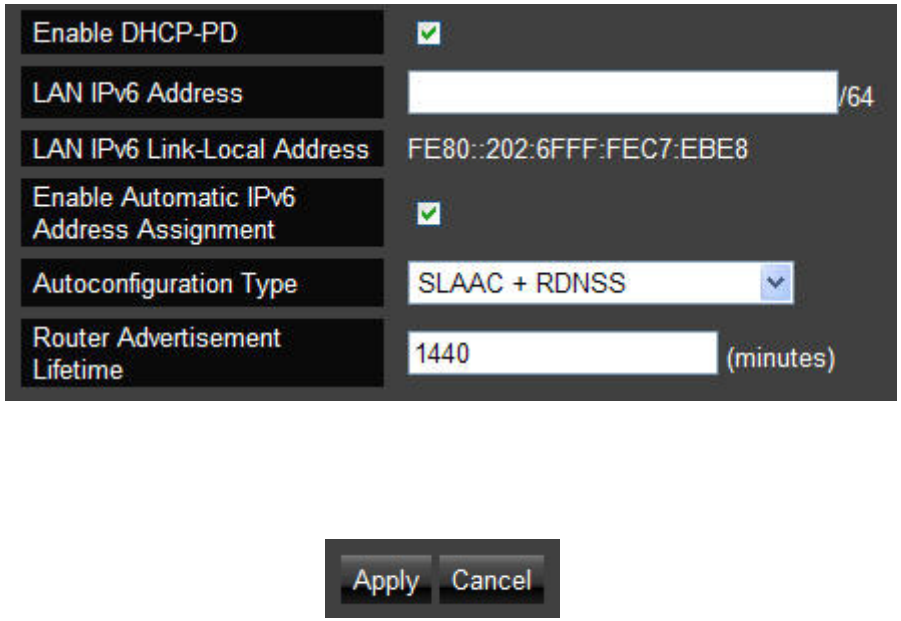
6.6.1 Configure PPPoE

- **Address Mode** Select Static if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select Dynamic.
- **IP Address** Enter the IP address (Static PPPoE only).
- **User Name** Enter your PPPoE user name.
- **Password** Enter your PPPoE password.
- **Verify Password** Retype the your PPPoE password.
- **Service Name** Enter the ISP Service Name (optional).
- **Reconnect Mode** Select either Always-on, On-Demand, or Manual.
- **Maximum Idle Time** Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.
- **MTU** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.
- **Obtain A DNS Server Address Automatically** Enable or disable obtaining a DNS server automatically.
- **Primary IPv6 DNS Address** Enter the primary IPv6 DNS address.
- **Secondary IPv6 DNS Address** Enter the secondary IPv6 DNS address.



- **Enable DHCP-PD** Enable or disable DHCP-prefix delegation (PD).
- **LAN IPv6 Address** Enter the LAN IPv6 address.
- **LAN IPv6 Link-Local Address** Enter the LAN IPv6 link-local address.
- **Enable Automatic IPv6 Address Assignment** Enable or disable automatic IPv6 address assignment.
- **Autoconfiguration Type** Enter the autoconfiguration type. (Default: `SLAAC +RDNSS`)
- **Router Advertisement Lifetime** Enter the IPv6 Address Lifetime (in minutes).

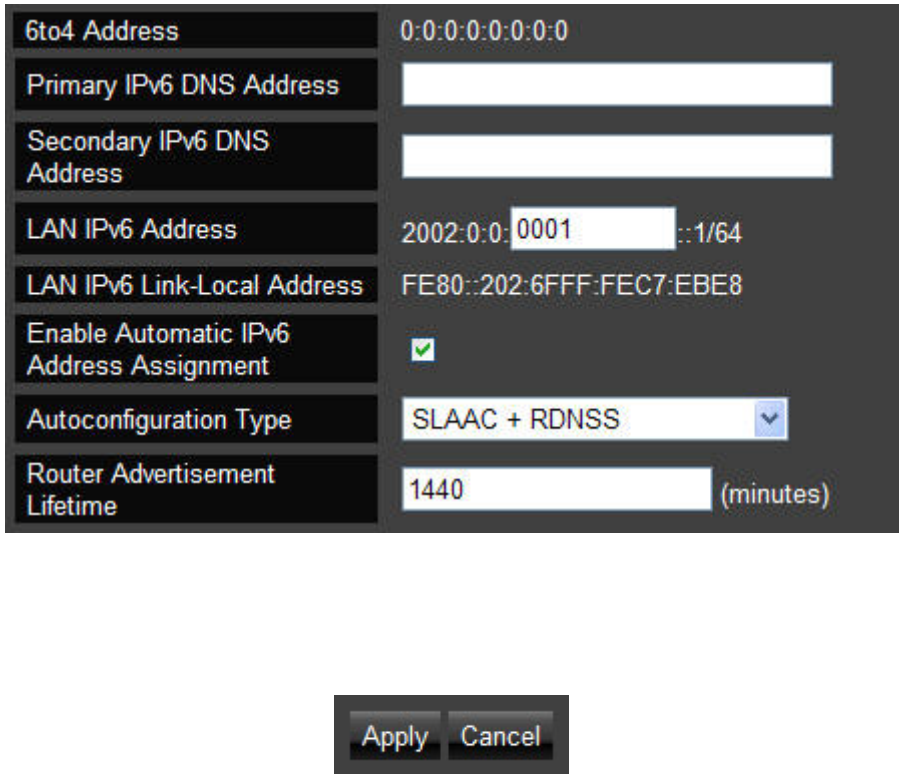
Click `Apply` to save the settings or `Cancel` to discard changes.



6.6.1 Configuring 6to4

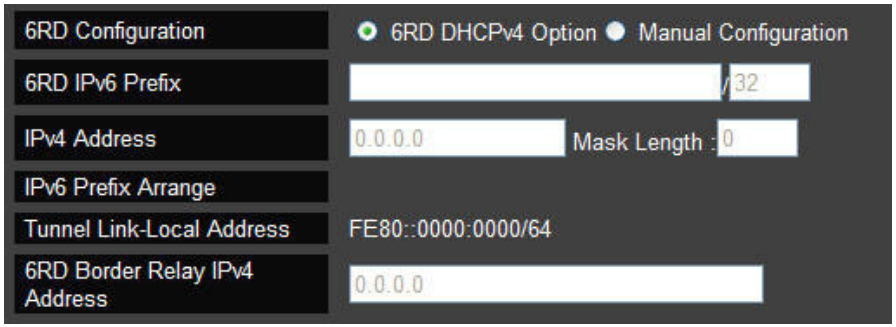
- **6to4 Address** Enter the 6to4 IP address.
- **Primary IPv6 DNS Address** Enter the primary IPv6 DNS address.
- **Secondary IPv6 DNS Address** Enter the secondary IPv6 DNS address.
- **LAN IPv6 Address** Enter the LAN IPv6 address.
- **LAN IPv6 Link-Local Address** Enter the LAN IPv6 link-local address.
- **Enable Automatic IPv6 Address Assignment** Enable or disable automatic IPv6 address assignment.
- **Autoconfiguration Type** Enter the autoconfiguration type. (Default: `SLAAC +RDNSS`)
- **Router Advertisement Lifetime** Enter the IPv6 Address Lifetime (in minutes).

Click `Apply` to save the settings or `Cancel` to discard changes.



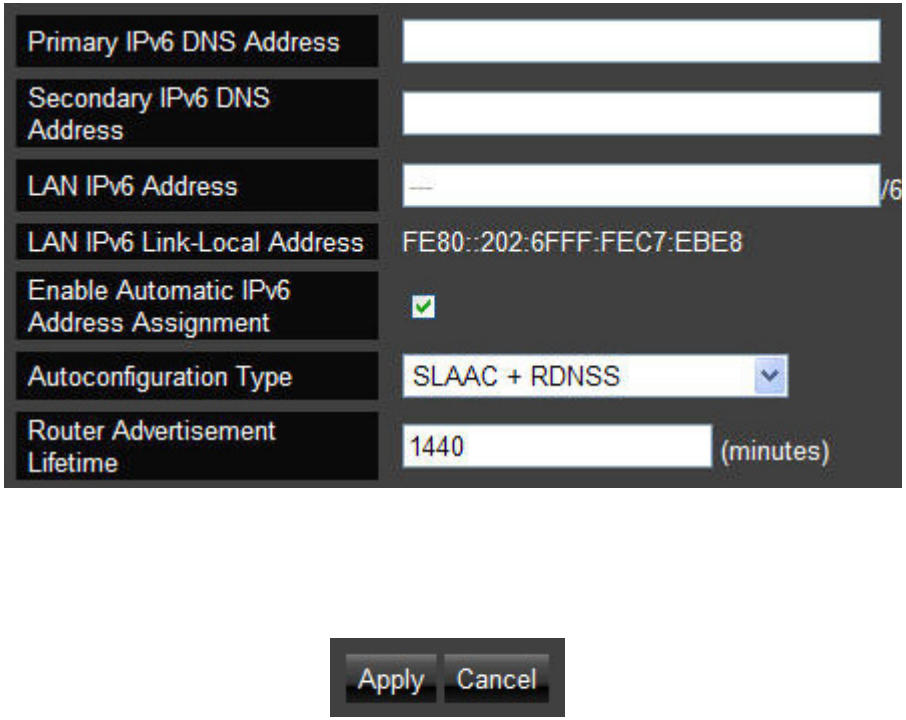
6.6.1 Configure 6RD

- **6RD Configuration** Enable `6RD DHCPv4 Option` or `Manual Configuration`
- **6RD IPv6 Prefix** Enter the 6RD IPv6 prefix.
- **IPv4 Address** Enter the IPv4 address.
- **Mask Length** Enter the IPv4 address mask length.
- **IPv6 Prefix Arrange** Enter the IPv6 prefix arrange.
- **Tunnel Link-Local Address** Enter the tunnel link-local address.
- **6RD Border Relay IPv4 Address** Enter the 6RD border relay IPv4 address.



- **Primary IPv6 DNS Address** Enter the primary IPv6 DNS address.
- **Secondary IPv6 DNS Address** Enter the secondary IPv6 DNS address.
- **LAN IPv6 Address** Enter the LAN IPv6 address.
- **LAN IPv6 Link-Local Address** Enter the LAN IPv6 link-local address.
- **Enable Automatic IPv6 Address Assignment** Enable or disable automatic IPv6 address assignment.
- **Autoconfiguration Type** Enter the autoconfiguration type. (Default: `SLAAC +RDNSS`).
- **Router Advertisement Lifetime** Enter the IPv6 Address Lifetime (in minutes).

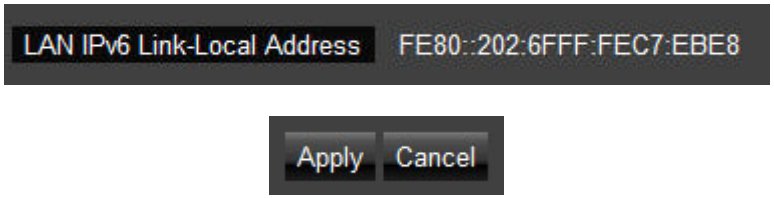
Click `Apply` to save the settings or `Cancel` to discard changes.



6.6.1 Configure Link-Local

LAN IPv6 Link-Local Address Enter the LAN IPv6 link-local address.

Click `Apply` to save the settings or `Cancel` to discard changes.



6.7 Firewall Setup

6.7.1 Configure Basic Settings

The ESR9850v2 firewall automatically detects and blocks Denial of Service (DoS) attacks. URL blocking, packet filtering and stateful packet inspection (SPI) are also supported. The details of the attack and the timestamp are recorded in the security log.

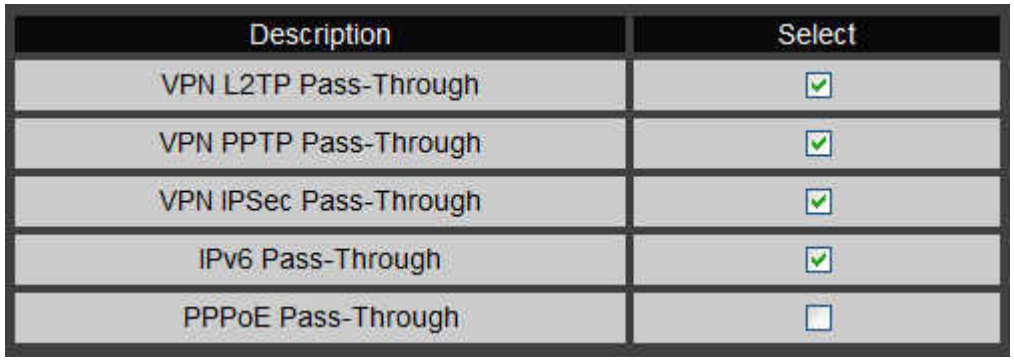
Firewall Enable or disable the firewall of the ESR9850v2.

Click `Apply` to save the settings or `Cancel` to discard changes.

6.7.1 Configuring Advanced Settings

The router supports VPN pass-through which allows virtual private networking (VPN) packets to pass through the firewall.

- **VPN L2TP Pass-through** Click `Select` to allow an L2TP connection method over a VPN.
- **VPN PPTP Pass-through** Click `Select` to allow a PPTP connection method over a VPN.
- **VPN IPSec Pass-through** Click `Select` to allow an IPSec connection method over a VPN.
- **IPv6 Pass-through** Click `Select` to allow IPv6 packets to pass through the firewall.
- **PPPoE Pass-through** Click `Select` to allow a PPPoE packets to pass through the firewall.



Click `Apply` to save the settings or `Cancel` to discard changes.

Note:
VPN L2TP Pass-through, VPN PPTP Pass-through, and VPN IPSec Pass-through are enabled by factory default.

6.7.1 Configuring Demilitarized Zone

Configuring a device on the LAN as a demilitarized zone (DMZ) host allows unrestricted two-way Internet access for Internet applications, such as online video games, to run from behind the NAT firewall. The DMZ function allows the router to redirect all packets going to the WAN port IP address to a particular IP address on the LAN. The difference between the virtual server and the DMZ function is that a virtual server redirects a particular service or Internet application, such as FTP, to a particular LAN client or server, whereas a DMZ redirects all packets, regardless of the service, going to the WAN IP address to a particular LAN client or server.

A DMZ host allows a computer to have all its connections and ports completely open during data transmission.

WARNING!
The PC defined as a DMZ host is not protected by the firewall and is vulnerable to malicious network attacks. Do not store or manage sensitive information on the DMZ host.

- **Enable DMZ** Click `Enable DMZ` to activate DMZ functionality.
- **Local IP Address** Enter an IP address of a device on the LAN.

Click `Apply` to save the settings or `Cancel` to discard changes.

6.7.1 Configuring Denial of Service

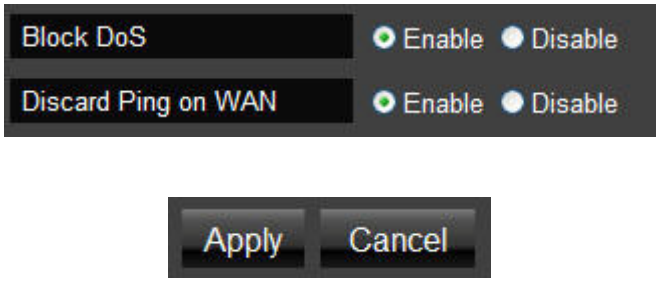
To enable blocking of denial of service (DoS) attacks, select the DoS option in the Firewall section.

DoS attacks can flood the internet connection with the continuous transmission of data. Blocking these attacks ensures that the internet connection is always available.

WAN Settings

- **Block DoS** Enable or disable blocking DoS attacks.
- **Discard Ping on WAN** ICMP (ping) packages are blocked while `Block DoS` is enabled. Enable `Discard Ping on WAN` if the WAN port is required.

Click `Apply` to save the settings or `Cancel` to discard changes.



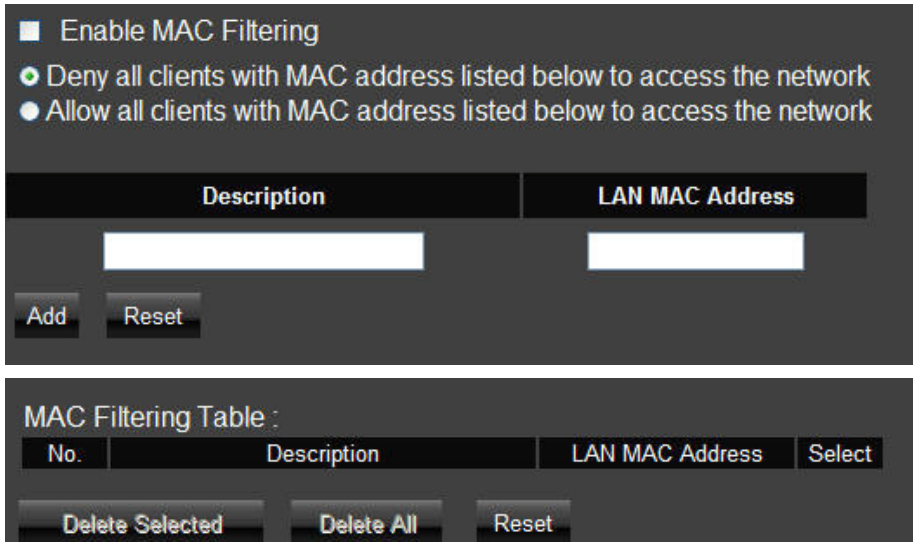
6.7.1 Configure MAC Filter

MAC Filters are used to deny or allow LAN computers from accessing the Internet.

- **Enable MAC Filtering** Enable or disable MAC filtering.
- **Deny/Allow all clients with MAC address listed below to access the network**
- **Description** Enter a description for a LAN MAC address.
- **LAN MAC Address** Enter the LAN MAC address.
- Click `Add` to add a device to the *MAC Filtering Table* or `Reset` to abort the process.

View and select devices in the *MAC Filtering Table.*

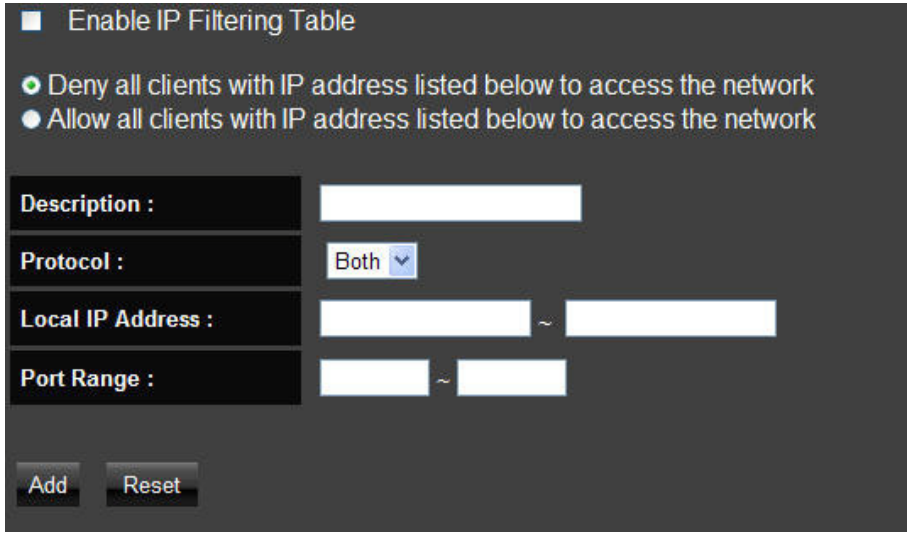
Click `Delete Selected` or `Delete All` to remove devices from the table. Click Reset to abort.



6.7.1 Configure IP Filter

IP Filters are used to deny or allow LAN computers from accessing the Internet.

- **Enable IP Filtering** Enable or disable IP filtering.
- **Deny/Allow all clients with IP address listed below to access the network**
- **Allow all clients with IP address listed below to access the network**
- **Description** Enter a description for a LAN IP address.
- **Protocol** Select `TCP`, `UDP` or `Both`.
- **Local IP Address** Enter the local IP address range.
- **Port Range** Enter the local port range.
- Click `Add` to add a device to the *IP Filtering Table* or `Reset` to abort the process.



View and select devices in the *IP Filtering Table.*

Click `Delete Selected` or `Delete All` to remove devices from the table. Click Reset to abort.

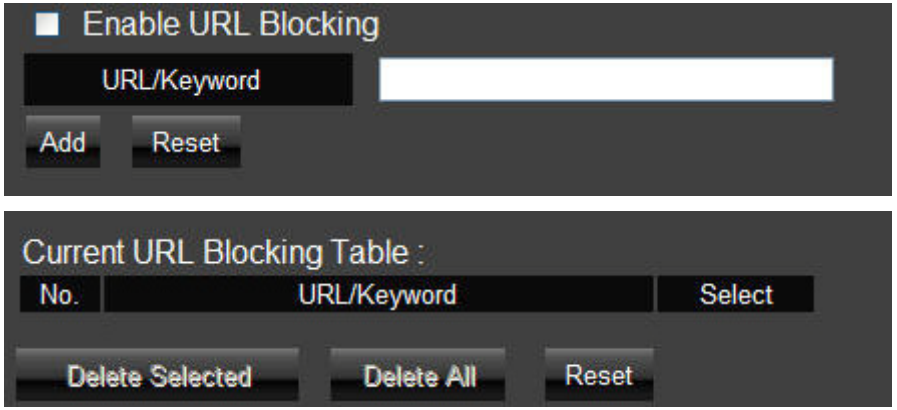
6.7.1 URL Filtering

You can block access to certain Web sites for a particular PC by entering either a full URL address or just a keyword of the Web site.

- **Enable URL Blocking** Enable or disable URL blocking.
- **URL/Keyword** Enter a URL or keyword to filter on.
- Click `Add` to add a device to the *URL Blocking Table* or `Reset` to abort the process.

View and select devices in the *URL Blocking Table.*

Click `Delete Selected` or `Delete All` to remove devices from the table. Click Reset to abort.

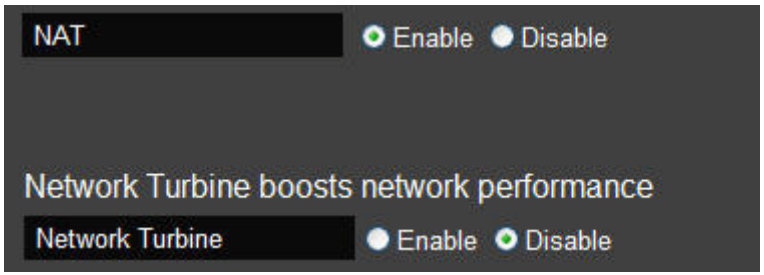


6.8 Advanced Network Settings

6.8.1 NAT Setup

Network address translation (NAT) allows users on the LAN to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides firewall protection from hacker attacks and allows for mapping LAN IP addresses to WAN IP addresses with key services such as websites, FTP, video game servers, etc.

- **NAT** `Enable` or `Disable` the NAT.
- **Network Turbine** `Enable` or `Disable` the network turbine.



Note:
The network turbine is designed to improve the router's performance. There is about 20~30% improvement when the network turbine is enabled.

Note:
The network turbine may cause problems with the Internet connection. Disable the network turbine function if you experience connection issues.

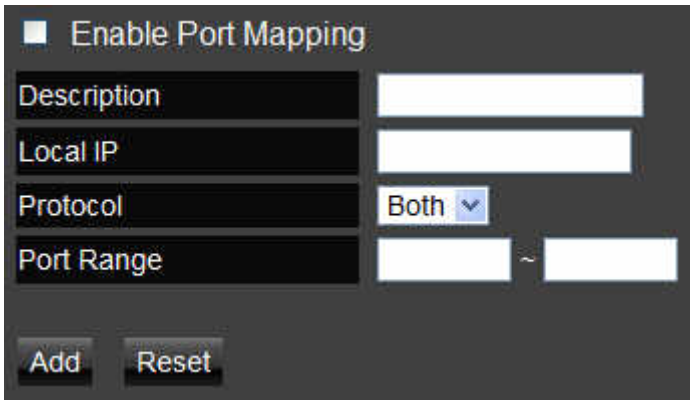
Click `Apply` to save the settings or `Cancel` to discard changes.

6.8.1 Port Mapping Setup

Port Mapping allows you to redirect a particular range of service port numbers from the WAN to a particular LAN IP address.

- **Enable Port Mapping** Click `Enable Port Mapping` to activate port mapping.
- **Description** Enter notes or details about the mapped port range configuration.
- **Local IP** Enter the local IP address of the server behind the NAT firewall.
- **Protocol** Select the protocol to use for mapping from the following: `TCP`, `UDP` or `Both`.
- **Port Range** Enter the range of ports to be forwarded.

Click `Add` to append a new device to the list or `Reset` to discard changes.



Current Port Mapping Table

Displays a list of mapped port ranges in use on the network.

- **No.** The sequence number of the mapped port range.
- **Description** Notes or details about the mapped port range.
- **Local IP** IP address of the server for the mapped port range.
- **Type** The protocol used to communicate with the WAN ports and LAN server.
- **Port Range** The range of mapped ports.
- **Select** Indicates the device(s) that can have actions performed on them.

Click `Delete Selected` to remove selected devices from the list.

Click `Delete All` to remove all devices form the list.

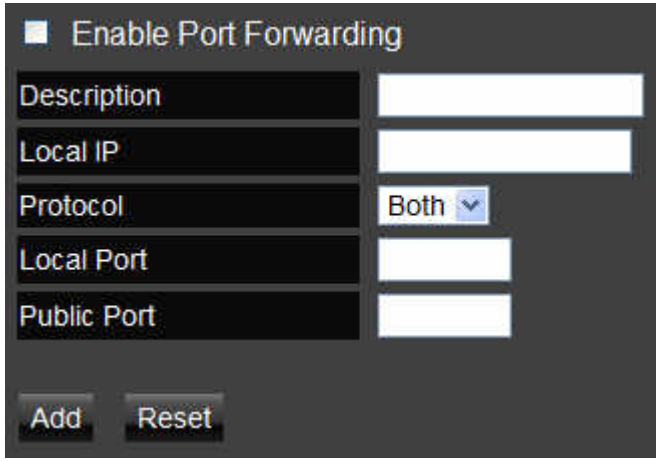
Click `Reset` the discard changes.

Click `Apply` to save the settings or `Cancel` to discard changes.

6.8.1 Port Forwarding Setup

Port forwarding enables multiple server applications on a LAN to serve clients on a WAN over a single WAN IP address. The router accepts incoming client packets, filters them based on the destination WAN, or public, port and protocol and forwards the packets to the appropriate LAN, or local, port. Unlike the DMZ feature, port forwarding protects LAN devices behind the firewall.

- **Enable Port Forwarding** Click `Enable Port Forwarding` to active port forwarding.
- **Description** Enter notes or details about the forwarded port configuration.
- **Local IP** Enter the local IP address of the server behind the NAT firewall.
- **Protocol** Select the protocol to use for mapping from the following: `TCP`, `UDP` or `Both`.
- **Local Port** Enter the LAN port number that WAN client packets will be forward to.
- **Public Port** Enter the WAN port number that clients will send their packets to.



Click `Add` to append a new configuration to the table or `Reset` to discard changes.

Click `Apply` to save the settings or `Cancel` to discard changes.

Current Port Forwarding Table

The table of current port forwarding configurations.

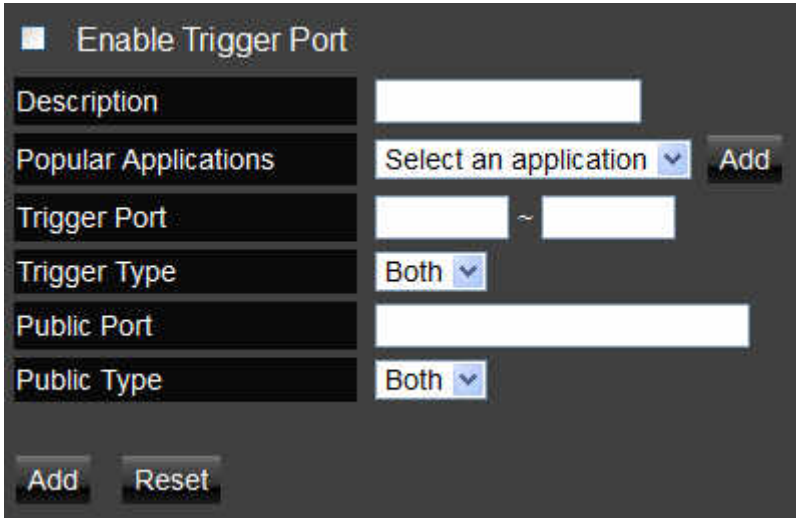
Click `Delete Selected` to remove selected devices from the list.

Click `Delete All` to remove all devices form the list.

Click `Reset` the discard changes.

6.8.1 Port Triggering Setup

Some applications, such as online games, videoconferencing and VoIP telephony, require multiple ports for inbound and outbound traffic. If an application requires both an incoming and an outgoing port simultaneously, it is possible to configure static port forwarding to handle the packets. That is not an optimal solution because a static IP address must be configured for each device. With port triggering an application, local port or range of ports and a communication protocol can be mapped to a specific public port. Sending packets out over the local port triggers the router to open an incoming local port that is mapped to the same public port and application as the outgoing local port(s). The local application can communicate over the incoming and outgoing ports without the need for creating a fixed address.



- **Enable Port Triggering** Click `Enable Trigger Port` to activate port triggering.
- **Description** Enter notes or details about the port triggered configuration.
- **Popular Applications** Select a default application or add a new one.
- **Trigger Port** Enter the application's outbound port number(s).
- **Trigger Type** Select the protocol to use for port triggering from the following: `TCP`, `UDP` or `Both`.
- **Public Port** Enter the inbound port(s) for the application in the following format: 2300-2400 or 47624.
- **Public Type** Select the protocol to use for the inbound port from the following: `TCP`, `UDP` or `Both`.

Click `Add` to append a new configuration to the table or `Reset` to discard changes.

Current Port Triggering Table

The list of current port triggering configurations.

Click `Delete Selected` to remove selected devices from the list.

Click `Delete All` to remove all devices form the list.

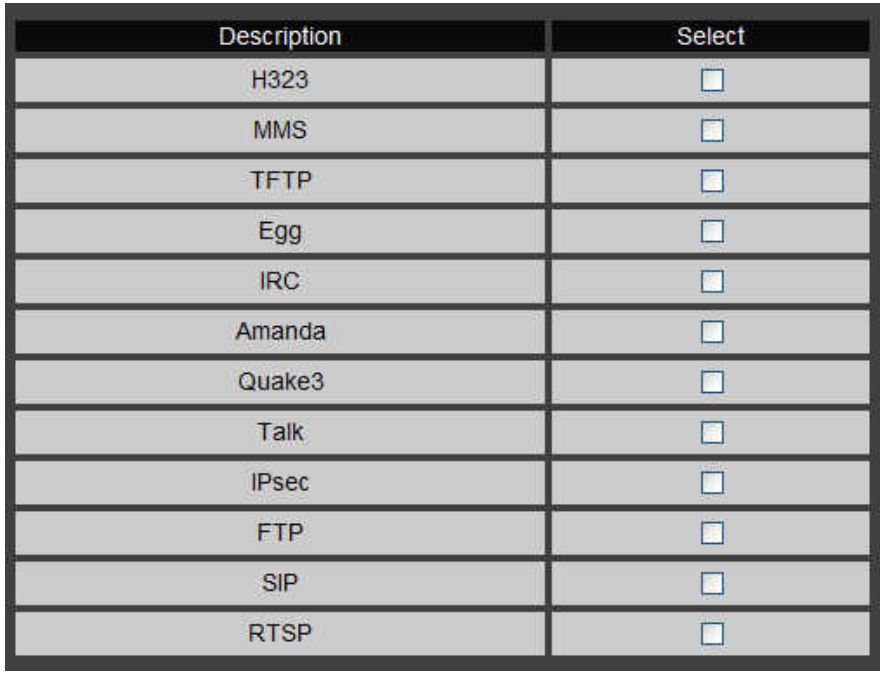
Click `Reset` the discard changes.

Click `Apply` to save the settings or `Cancel` to discard changes.

6.8.1 Application Layer Gateway Setup

The ALG (Application Layer Gateway) serves as a window between correspondent application processes so that they may exchange information on an open environment.

Select the listed applications that need ALG support and then the router will authorize them to pass through the NAT gateway.



Click `Apply` to save the settings or `Cancel` to discard changes.

6.8.1 Universal Plug and Play Setup

UPnP helps internet devices, such as gaming and videoconferencing, to access the network and connect to other registered UPnP devices.

Click `Enable` or `Disable` to activate or deactivate UPnP.

Click `Apply` to save the settings or `Cancel` to discard changes.

6.8.1 Internet Group Multicast Protocol Setup

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a multicast group.

Click `Enable` or `Disable` to activate or deactivate IGMP.

Note:
Disabling the Multicast function may cause IP based multi-media devices, such as an IP-STB or OTT box, may lose connectivity with the media streaming server.

Click `Apply` to save the settings or `Cancel` to discard changes.

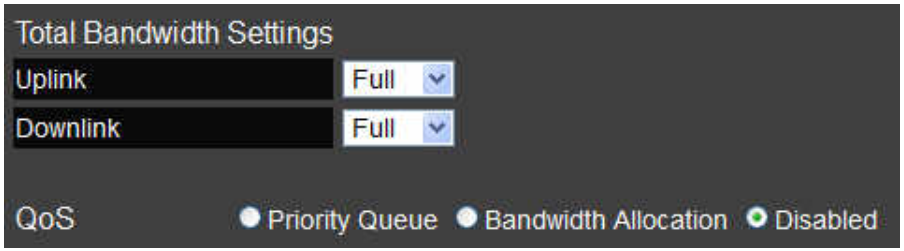
6.8.1 Quality of Service Setup

QoS can prioritize bandwidth use such as video streaming, online gaming, VoIP telephony and videoconferencing to ensure stable and efficient network performance.

Total Bandwidth Settings

Uplink Select the maximum bandwidth speed for outbound traffic.

Downlink Select the maximum bandwidth speed for inbound traffic.



Note:

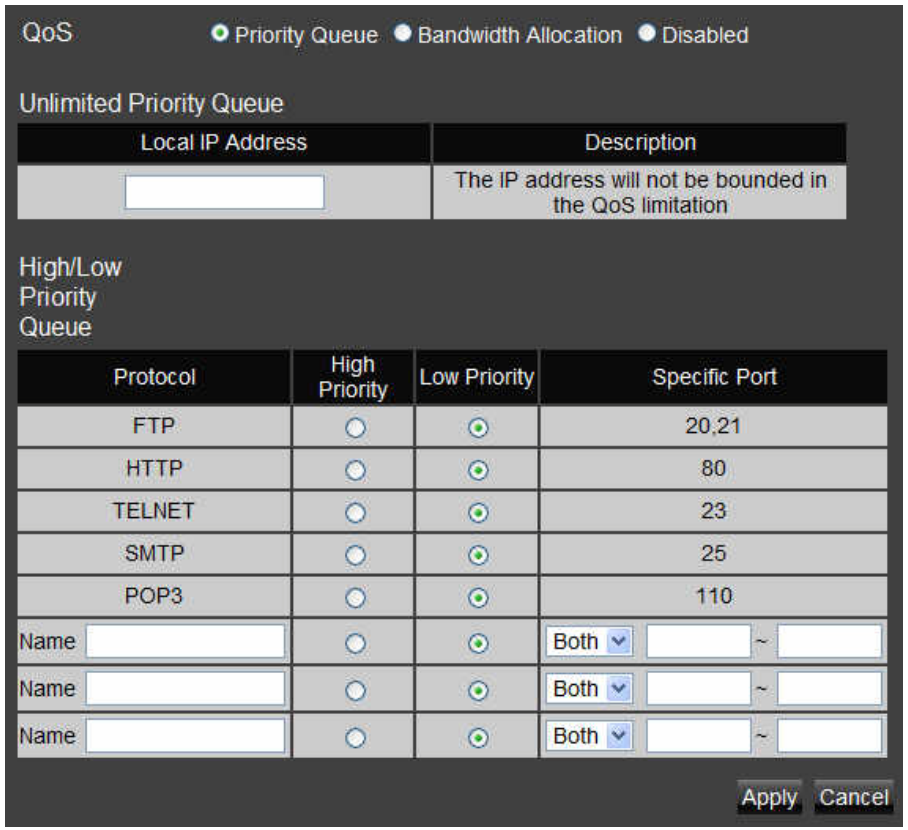
Click `Disabled` if you do not want to prioritize any data or protocol.

Priority Queue

Set network resource usage based on specific protocols or port ranges. Incoming packets are processed based on the protocols' position within the queue.

Unlimited Priority Queue

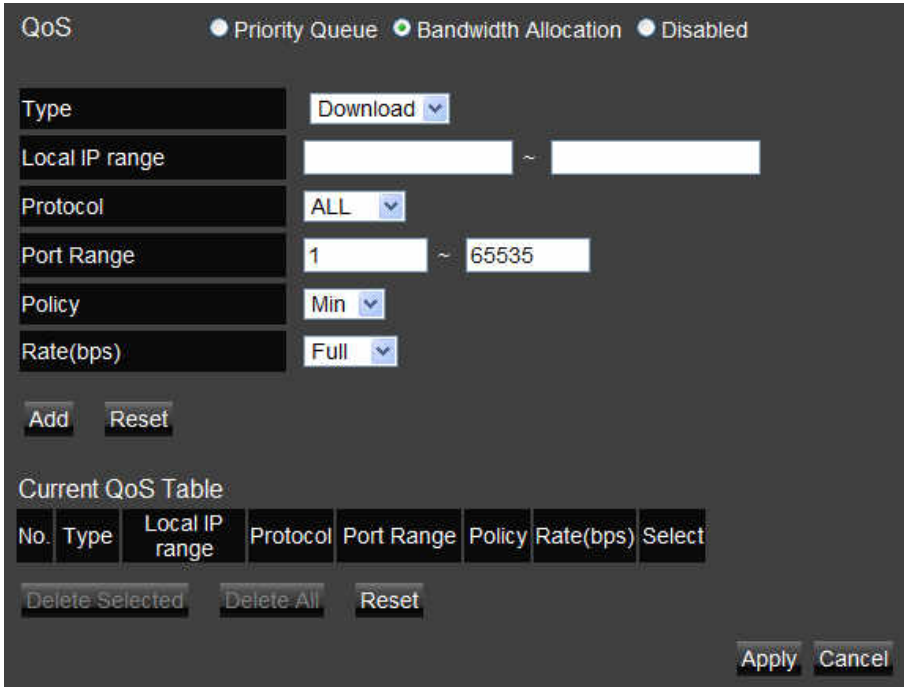
- **Local IP Address** Enter the local IP address of a device on the network. This device's activity is not restricted by the QoS feature.
- **High/Low Priority Queue:** Specify the priority for different protocols. Additional protocols and port ranges can be added.



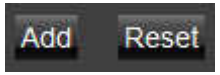
Bandwidth Allocation

Set network resource usage, for inbound and outbound traffic, based on local IP and port ranges.

- **Type** Select `Download` or `Upload` to specific the direction of packet traffic.
- **Local IP Range** Enter the local IP range of the current configuration.
- **Protocol** Select the protocol to manage for the current configuration.
- **Port Range** Enter the local port range of the current configuration.
- **Policy** Select `Min` or `Max` to specify the type of configuration policy.
- **Rate (bps):** Select the bandwidth rate, in bits per second (bps), of the current configuration.



Click `Add` to save the settings and list the configuration in the Current QoS table or `Reset` the discard changes.



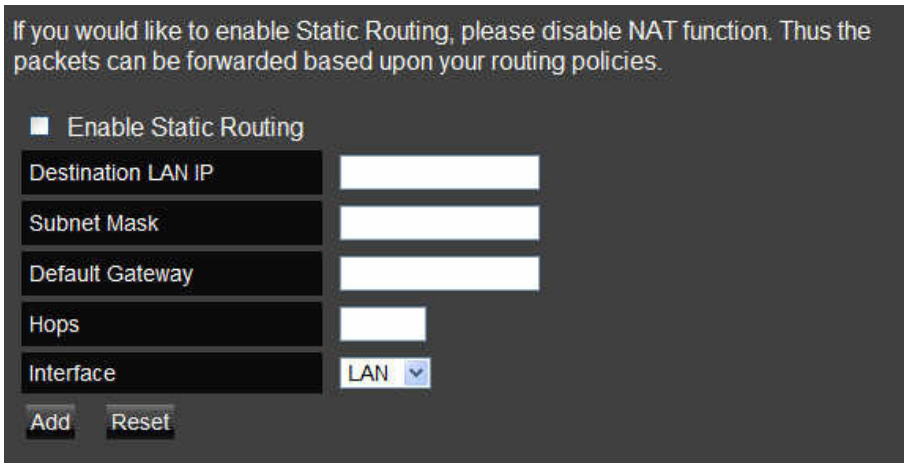
Click `Apply` to save the settings or `Cancel` to discard changes.

6.8.1 Routing Setup

Typically static routing does not need to be setup because the ESR9850v2 has adequate routing information after it has been configured for Internet access. Static routing is only necessary if the router is connected to network under a different subnets.

Note:
To enable a static routing, NAT must be disabled.

If the router is connected with a network under the different subnet, the routing setup allows the network connection within two different subnets.



- **Enable Static Routing** Click `Enable Static Routing` to activate the feature.
- **Destination LAN IP** Enter the LAN IP address of the destination device.
- **Subnet Mask** Enter the Subnet Mask of the destination device.
- **Default Gateway** Enter the default gateway IP address for the destination device.
- **Hops** Enter the maximum number of hops within the static routing that a packet is allowed to travel.
- **Interface** Select LAN or WAN as the interface.

Click `Add` to save the settings and list the configuration in the Current Static Routing table or `Reset` the discard changes.

View and select devices in the *Current Static Routing Table.*

Click `Delete Selected` or `Delete All` to remove devices from the table. Click Reset to abort.

Click `Apply` to save the settings or `Cancel` to discard changes.

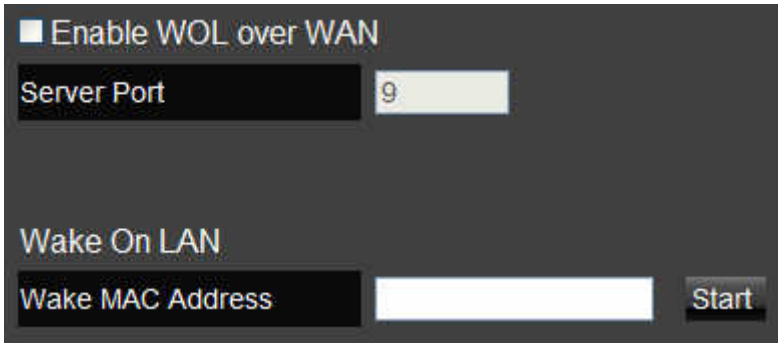
6.8.1 Wake on LAN Setup

Wake on LAN setup (WOL) allows the administrator to activate a computer over the network.

Enable WOL over WAN Click `Enable WOL over WAN` to activate the feature.

Server Port Enter the server port of the device to activate.

Wake MAC Address Enter the MAC address of the device to activate. Click `Start` to activate the device.

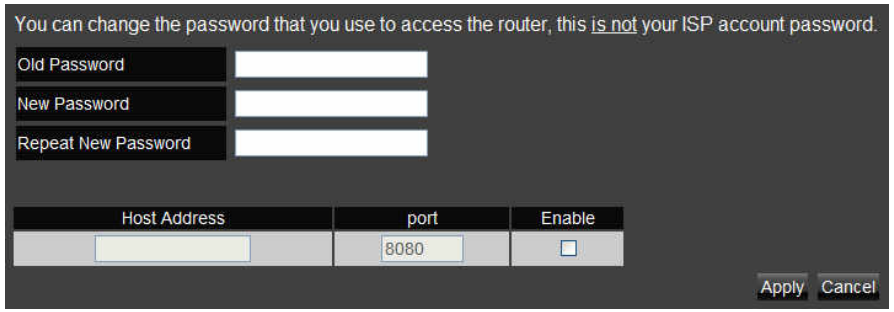


Click `Apply` to save the settings or `Cancel` to discard changes.

6.9 Tools Setup

6.9.1 Configuring the Administrator Account

Change the router's system password as well as setup a device to remotely configure the settings.



- **Old Password:** Enter the existing administrator password.
- **New Password:** Enter the new administrator password.
- **Repeat New Password:** Re-type the new administrator password.
- **Remote Management**
- **Host Address:** Enter the designated host IP Address.
- **Port:** Enter the port number (Default: **8080**) for remote accessing management web interface.
- **Enable:** Select to enable remote management.

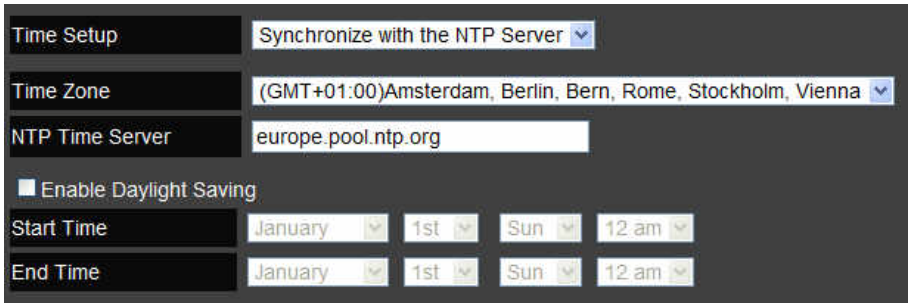
Click `Apply` to save the settings or `Cancel` to discard changes.

Note:
To access the settings of the ESR9850v2 remotely, enter the router's WAN IP address and port number.

6.9.1 Configuring the Router's Time

Change the system time of the ESR9850v2 and setup automatic updates through a network time protocol server (NTP).

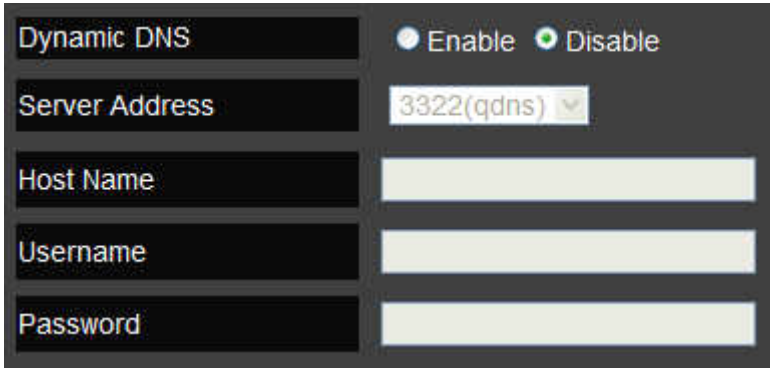
- **Time Setup** Select how the router obtains the current time.
- **Time Zone** Select the time zone for the router.
- **NTP Time Server** Enter the domain name or IP address of an NTP server.
- **Enable Daylight Saving** Click to enable or disable daylight savings time.
- **Start Time** Select the date and time when daylights savings time starts.
- **End Time** Select the date and time when daylights savings time ends.



6.9.1 Configuring DDNS

Dynamic Domain Name Service (DDNS) allows the administrator to map a static domain name to a dynamic IP address. A DDNS service provider, such as DynDNS, ZoneEdit or CyberGate, must provide an account, password, and static domain name to use this feature. DDNS particularly benefits end users that have their own websites or FTP sites.

- **Dynamic DNS** Enable or Disable DDNS.
- **Server Address** Select the DDNS Server Address.
- **Host Name** Enter the DDNS provider static domain name.
- **Username** Enter the username given by the DDNS provider.
- **Password** Enter the password given by the DDNS provider.



6.9.1 Diagnosing a Network Connection

The diagnosis feature allow the administrator to verify that another device is available on the network and is accepting request packets. If the ping result returns `alive`, it means a device is on line. This feature does not work if the target device is behind a firewall or has security software installed.

- **Address to Ping** Enter IP address of the device to ping.
- **Ping Result** View the result message from the ping test.

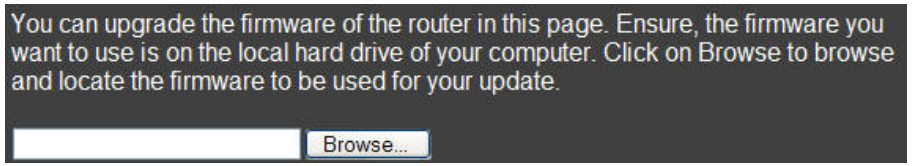
6.9.1 Upgrading Firmware

Firmware is system software that operates and allows the administrator to interact with the router.

WARNING!
Upgrading firmware through a wireless connection is not recommended. Firmware upgrading must be performed while connected to an Ethernet (LAN port) with all other clients disconnected.

To update the firmware version, follow these steps:

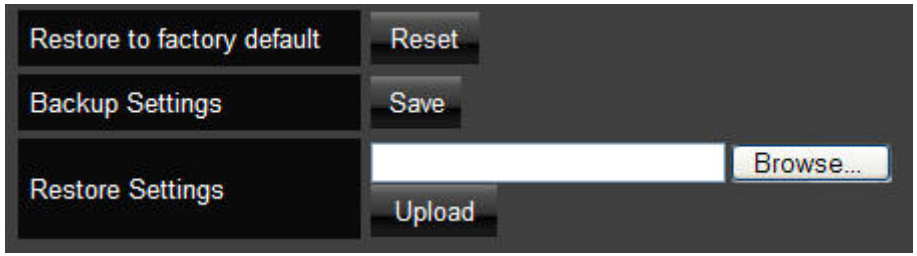
1. Download the appropriate firmware approved by EnGenius Networks from an approved web site.
2. Click `Browse`.
3. Browse the file system and select the firmware file.
4. Click `Apply`.


You can upgrade the firmware of the router in this page. Ensure, the firmware you want to use is on the local hard drive of your computer. Click on Browse to browse and locate the firmware to be used for your update.
Browse...

6.9.1 Backing Up Settings

Store multiple settings versions by saving the settings to a configuration file on the device.

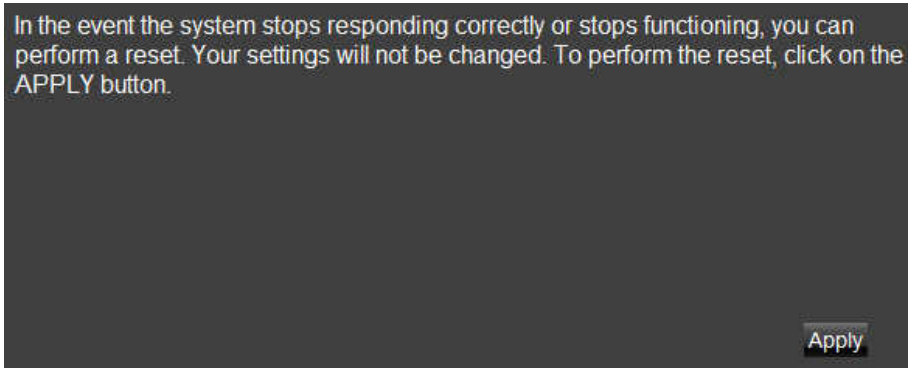
- **Restore to factory default** Click `Reset` to restore the ESR9850v2 to factory defaults.
- **Backup Settings** Click `Save` to save the current configuration on the ESR9850v2 to a *.dlf file.
- **Restore Settings** To restore saved settings, do the following:
  a. Click `Browse`.
  b. Browse the file system for location of the settings file (*.dlf).
  c. Click `Upload`.



6.9.1 Rebooting the Device

This feature allows the administrator to reboot the router in the event of a system hang up.

Click `Apply` to reset the device.


In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button.
Apply

Appendix A

6.1 Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

WARNING!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement

Important:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Appendix B

6.1 Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Important:

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Appendix C

6.1 Link Layers

There are different ways of connecting your personal computer (PC) or mobile computing device to the Internet. Here are four of the most common ways and how to connect to the Internet using them.

Dynamic IP Address (DHCP)

A DHCP of connection is where your internet connection is usually always on and your internet service provider automatically provides you with an IP address. A DHCP connection is usually from a Cable internet service.

Static IP

To set up a Static IP connection, enter the following: IP Address of the Internet Connection, Subnet Mask, Default Gateway, and both DNS Servers. This information can be obtained by either your Internet Service provider or Network Administrator. If your internet service provider requires a username and password to connect, you will then be prompted to enter the correct information.

MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for internet transmission. The factory default MTU size of Static IP is 1500. If you wish to manually change the MTU size, set it between 512 and 1500.

Point-to-Point Protocol over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE): To set up a PPPoE connection, enter the Username, Password, and Service (name) of the internet connection provided by your ISP. Click Next and the ESR300H should connect to the internet successfully. A PPPoE connection is usually from a DSL internet service.

1. Login: The username or e-mail address that the internet connection uses to access internet connectivity.
2. Password: The password that corresponds to the username or e-mail address used to connect to the internet in the PPPoE.
3. Service Name: The Service Name is optional. This is to signify the name of the Internet Service Provider.
4. MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for internet transmission. The factory default MTU size of Static IP is 1500. If you wish to manually change the MTU size, set it between 512 and 1500.
5. Point-to-Point Tunneling Protocol (PPTP)

To set up a PPTP connection, enter the type of WAN connection (Static IP or DHCP). After, depending on the type of WAN, follow the instructions of DHCP or Static IP to fill out the corresponding information. Then, proceed to enter the Username, Password, Service, and Connection ID of the PPTP internet connection. Once completed, click Next. Once configured, the internet connection will successfully connect.

Layer 2 Tunneling Protocol (L2TP)

To set up an L2TP connection, enter the type of WAN connection (Static IP or DHCP). After, depending on the type of WAN, follow the instructions of DHCP or Static IP to fill out the corresponding information. Then, proceed to enter the Username, Password, and Service. Click next when completed. Once configured, the internet connection will successfully connect.

MTU: Maximum Transmission Unit. It specifies the largest packet size permitted for internet transmission. The factory default MTU size of Static IP is 1500. If you wish to manually change the MTU size, set it between 512 and 1500.

Appendix D

6.1 WorldWide Technical Support

REGION/COUNTRY OF PURCHASE	SERVICE CENTRE		SERVICE INFORMATION
Canada	CANADA	web site	www.engeniuscanada.com
		email	rma@engeniuscanada.com
		contact numbers	Toll Free: (+1) 888-397-2788 Local: (+1) 905-940-8181
		hours of operation	Monday - Friday 9:00AM to 5:30PM EST (GMT-5)
USA	LOS ANGELES, USA	web site	www.engeniustech.com
		email	support@engeniustech.com
		contact numbers	Toll Free: (+1) 888-735-7888 Local: (+1) 714-432-8668
		hours of operation	Monday - Friday 8:00 AM to 4:30 PM PST (GMT-8)
Mexico, Central and Southern America	MIAMI, USA	web site	[ES] es.engeniustech.com [PT] pg.engeniustech.com
		email	miamisupport@engeniustech.com

REGION/COUNTRY OF PURCHASE	SERVICE CENTRE		SERVICE INFORMATION
		contact numbers	Miami: (+1) 305-887-7378 Sao Paulo, Brazil: (+55)11-3957-0303 D.F., Mexico:(+52)55-1163-8894
		hours of operation	Monday - Friday 8:00 AM to 5:30PM EST (GMT-5)
Europe	NETHERLANDS	web site	www.engeniusnetworks.eu
		email	support@engeniusnetworks.eu
		contact numbers	(+31) 40-8200-887
		hours of operation	Monday - Friday 9:00 AM - 5:00 PM (GMT+1)
Africa Middle East Russia CIS / Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Turkmenistan, Ukraine, Uzbekistan Turkey Afghanistan Pakistan Bangladesh, Maldives, Nepal, Bhutan, Sri Lanka	DUBAI, UAE	web site	www.engenius-me.com
		email	support@engenius-me.com
		contact numbers	Toll Free: U.A.E.: 800-EnGenius 800-364-364-87 General: (+971) 4357-5599
		hours of operation	Sunday - Thursday 9:00 AM - 6:00 PM (GMT+4)

REGION/COUNTRY OF PURCHASE	SERVICE CENTRE		SERVICE INFORMATION
Singapore, Cambodia, Indonesia, Malaysia, Thailand, Philippines, Vietnam China, Hong Kong, Korea India South Africa Oceania	SINGAPORE	web site	www.engeniustech.com.sg/e_warranty_form
		email	techsupport@engeniustech.com.sg
		contact numbers	Toll Free: Singapore: 1800-364-3648
		hours of operation	Monday - Friday 9:00 AM - 6:00 PM (GMT+8)
Others	TAIWAN, R.O.C.	web site	www.engeniusnetworks.com
		email	technology@senao.com

Note:

* Service hours are based on the local time of the service center.

* Please visit the website for the latest information about customer service.